Bachelorthesis

Erarbeitung eines Konzeptes zur aktiven Steuerung einer hochzuverlässigen Leistungsversorgungseinheit für ein hybrides Navigationssystem

Autor:
Lars Johannsen

Abgabedatum 13.07.2015

Erarbeitung eines Konzeptes zur aktiven Steuerung einer hochzuverlässigen Leistungsversorgungseinheit für ein hybrides Navigationssystem

Bachelorthesis

Hochschule Bremen
City University of Applied Sciences
Fakultät 4 - Elektrotechnik und Informatik
Elektrotechnik - Fachrichtung Elektronik

HSB
Hochschule Bremen
City University of Applied Sciences

Lars Johannsen
Mat.-Nr.: 293480

Abgabedatum 13.07.2015

Erstprüfer
Prof. Dr.-Ing. Mirco Meiners
Hochschule Bremen
City University of Applied Sciences

Zweitprüfer
Dipl. -Ing. Ulrich Uffelmann
Hochschule Bremen
City University of Applied Sciences
Lehrbeauftragter

Betreuer am Institut
M.Eng. René Schwarz
Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)
Institut für Raumfahrtsysteme, Bremen

Lars Johannsen
Erarbeitung eines Konzeptes zur aktiven Steuerung einer hochzuverlässigen Leistungsversorgungseinheit für ein hybrides Navigationssystem
Bachelorthesis Elektrotechnik

Hochschule Bremen
City University of Applied Sciences
Neustadtswall 30
28199 Bremen

Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)
Institut für Raumfahrtsysteme
Robert-Hooke-Str. 7
28359 Bremen

Bearbeitungszeitraum: 15. Mai 2015 - 13. Juli 2015

Erklärung

Hiermit erkläre ich, die Bachelorthesis selbstständig und ohne fremde Hilfe verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt zu haben. Außerdem befinden sich in diesem Dokument keine DLR-internen Zeichnungen oder Schaltpläne, die nicht für die Öffentlichkeit bestimmt sind.

Datum der Unterschrift

Lars Johannsen
Autor

Vorwort

Mit Hilfe dieser schriftlichen Ausarbeitung soll der akademische Grad eines Bachelor of Engineering erreicht werden. Das Thema „Erarbeitung eines Konzeptes zur aktiven Steuerung einer hochzuverlässigen Leistungsversorgungseinheit für ein hybrides Navigationssystem“ entstand im Rahmen eines Pflichtpraktikums der Hochschule Bremen, welches am DLR-Institut für Raumfahrtsysteme in Bremen durchgeführt worden ist. Des Weiteren entspricht das gewählte Thema meinem Studienschwerpunkt und bietet somit eine Möglichkeit, die im Studium erworbenen Kenntnisse anzuwenden und zu erweitern.
Mein Dank gilt besonders Prof. Dr.-Ing. Mirco Meiners, der mir als Erstprüfer immer mit seinem Rat zur Seite stand. Ferner möchte ich mich bei M.Eng. René Schwarz und Dipl.-Ing. (FH) Fred Ohlendorf für die außerordentliche Unterstützung und Betreuung im DLR bedanken. Mein Dank gilt auch der Hans-Böckler-Stiftung, ohne die es nicht möglich gewesen wäre zu studieren. Ferner gilt mein Dank Dipl.-Ing. Ulrich Uffelmann, der sich bereit erklärte, im Prüfungsverfahren als Zweitprüfer zur Verfügung zu stehen. Abschließend danke ich den Helfern die sich bereit erklärt haben mir bei der Korrektur dieser Bachelorthesis zu helfen.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AK	Anforderungsklasse
ARP	Aerospace Recommended Practice (Luft- und Raumfahrtrichtlinien)
ASIC	application-specific integrated circuit (anwendungsspezifische integrierte Schaltung)
ASIL	Automotive Safety Integrity Level (Automobile Sicherheitsbereiche)
B.Eng.	Bachelor of Engineering
DAL	Design Assurance Level (Konstruktionssicherheitsebene)
DIN	Deutsches Institut für Normung
DLR	Deutsches Zentrum für Luft- und Raumfahrt
ECSS	European Cooperation for Space Standardization (Europäische Kooperation für Raumfahrtnormung)
EN	Europäische Normen
EUROCAE	European Organization for Civil Aviation Equipment (Europäische Organisation für zivile Flugausrüstung)
FMEA	Failure Mode and Effects Analysis (Fehlermöglichkeits- und -einflussanalyse)
FPGA	Field Programmable Gate Array (im Feld (also vor Ort, beim Kunden) programmierbare (Logik-)Gatter-Anordnung.)
FIT	Failure in Time (Ausfälle pro Zeiteinheit)
GNC	Guidance, Navigation and Control ((Flug-)Führung, Navigation und Regelung)
HNS	Hybrid Navigation System
IEC	International Electrotechnical Commission (Internationale Elektrotechnische Kommission)
LDO	Low-Drop-(Out) Spannungsregler
MTBF	Mean Time Between Failures (Mittlere Brauchbarkeitsdauer)
PCB	Leiterplatte (printed circuit board (Platine oder gedruckte Schaltung)
PCP	Peripheral Control Processor
PDU	power distribution unit (Leistungsversorgungseinheit)
PFH	Probability of dangerous failure per hour (Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde)
E/E/PE	Electrical/Electronic/Programmable Electronic (auch E/E/PES; elektrische/elektronische/programmierbare elektronischee Sicherheitssysteme)
REX	Returnable Experiment (Rückkehrexperiment)
RPZ	Risiko-Prioritätszahl
RTCA	Radio Technical Commission for Aeronautics (Technischer Funkausschuss für Flugwesen)
SAE	Society of Automotive Engineers (Verband der Automobilingenieure)

SHEFEX	Sharp Edge Flight Experiment (scharfkantiges Flugexperiment)
SIL	Safety Integrity Level (Sicherheitsbereiche)
TTL	Transistor-Transistor-Logik
UART	Universal Asynchronous Receiver Transmitter (universell verwendbarer asynchroner Empfänger Sender)
VDA	Verband der Automobilindustrie
WDC	Watchdog Counter (Elektronische Überwachungseinheit)

Abstract

Mit SHEFEX III verfolgt das Deutsche Zentrum für Luft- und Raumfahrt konsequent seine Forschungs- und Entwicklungsarbeiten im Rahmen des SHEFEX-Programms. SHEFEX III konzentriert sich auf die Aspekte von Navigation, Flugregelung, Bahnplanung und Kostenminimierung. Die Abteilung Guidance, Navigation and Control (GNC) am DLR-Institut für Raumfahrtsysteme in Bremen entwickelt ein hybrides Navigationssystem, sowie die Flugführung für diese Mission. In Hinblick auf nachfolgende Missionen soll bei der Entwicklung des Navigationssystems darauf hingewirkt werden, dass es auch für zukünftige Anwendungen verwendet werden kann. Damit dieses System hochzuverlässig und fehlertolerant ist, benötigt es eine ausfallsichere Leistungsversorgungseinheit (PDU). Um die Belastung der Energieversorgung beim Betrieb des Systems kontrollieren und überwachen zu können, soll die PDU mit einer aktiven Steuerung ausgestattet werden, die es ermöglicht, flexibel auf auftretende Fehlerzustände reagieren zu können.

In der vorliegenden Bachelorthesis wird ein Konzept zur hochzuverlässigen Steuerung der Leistungsversorgungseinheit für das SHEFEX III-Navigationssystem erarbeitet. Zu diesem Zweck werden verschiedene Verfahren und Normen untersucht, miteinander verglichen und deren Anwendbarkeit für SHEFEX III überprüft.

Dieses Konzept dient dem DLR anschließend dazu, eine PDU-Steuerung zu entwerfen und zu implementieren.

Diese Thesis entstand im Rahmen eines studienbezogenen Praktikums und der anschließenden Fortführung des Projektes als studentische Hilfskraft. Die Thesis wurde der Hochschule Bremen als Bachelorthesis vorgelegt, um den akademischen Grad eines Bachelor of Engineering (B.Eng.) zu erreichen.

1 Einleitung

Seit Beginn der Menschheit üben die Sterne eine enorme Faszination auf den Menschheit aus. Schon vor circa 4000 Jahren versuchten Menschen die Gestirne darzustellen und zu erforschen, wie die Himmelsscheibe von Nebra beweist. Mittlerweile ist der Bereich um die Weltraumforschung schon weit vorangeschritten. Es wurde in der Vergangenheit bereits Großes geleistet, um den Weltraum besser zu verstehen. Darüber hinaus ist davon auszugehen, dass die Forschung weiter rasant voranschreiten wird. Die Probleme bei der modernen Raumfahrt sind immer häufiger weniger technischer Natur sondern finanzieller Art. Ein Beispiel für die schwierige Finanzierungslage ist der Betrieb der ISS und die Finanzierung einer möglicherweise bemannten Marslandung. Immer häufiger ist es notwendig, Unternehmen aus der Privatwirtschaft in Entwicklungen mit einzubeziehen [23]. Dieses Vorgehen schafft auf der einen Seite eine Budgetentlastung, bringt aber auch neue Probleme, wie z.B. Fragen der Haftung. Ein Beispiel dafür ist die Explosion einer Antares-Rakete im Oktober 2014. Bislang ist noch nicht klar, wer die Kosten für die Reparatur des durch die Explosion entstandenen Schaden tragen muss [28].
Die DLR Mission SHEFEX, versucht mit neuen Ansätze in der Auslegung und Konstruktion von Flugkörpern auf die aktuellen Anforderungen zu reagieren. Nach den ersten beiden erfolgreichen Missionen SHEFEX I und SHEFEX II wurde beschlossen diese Erfolgsgeschichte mit SHEFEX III fortzusetzen. Die Schwerpunkte bei der SHEFEX III-Mission liegen in der Flugführung, Navigation und Flugregelung, sowie auf Bahnplanung, Funktionalitätsuntersuchungen, Kostenminimierung, Systems Engineering und Skalierbarkeit in Hinblick auf die bevorstehende Entwicklung des REX-Free-Flyers. Nach Abschluss des SHEFEX-Programmes wird die Entwicklung des REX-Free-Flyers von den Missionsergebnissen profitieren. Der Rex-Free Flyer soll zukünftig eine kostengünstige und zuverlässige Plattform für unbemannte Experimente in der Schwerelosigkeit zur Verfügung stellen.
Ein wichtiger Bestandteil des SHEFEX-Projektes ist unter anderem, dass von der GNC-Abteilung zu entwickelnde hybride Navigationssystem. Dieses innovative und hochverfügbare Navigationssystem errechnet mit Hilfe verschiedener Sensoren (Drehraten- und Beschleunigungssensoren, Sonnensensoren, Sternkameras und GPS-Empfänger) fortlaufend die aktuelle Position und Lage des Flugkörpers. Im Kontext des SHEFEX III-Navigationssystems wird daher auch ein Referenzdesign für eine hochverfügbare Leistungsversorgungseinheit (englisch: power distribution unit, PDU) entwickelt. Die PDU stellt die von den internen und externen Komponenten des Navigationssystems benötigten Spannungsebenen in Form von unabhängig schaltbaren Kanälen bereit. Das Schalten dieser Kanäle ermöglicht ein geregeltes Hochfahren des Navigationssystems, Funktionstests der einzelnen Komponenten sowie eine Abschaltung von Komponenten im Fehlerfall, bedarf aber einer aktiven Steuerung.
Thesis beschäftigt sich nachfolgend mit der Erstellung eines Konzeptes zur Steuerung einer hochzuverlässigen Leistungsversorgungseinheit (PDU) für das SHEFEX III-Navigationssystem.

„Das Universum ist vollkommen. Es kann nicht verbessert werden. Wer es verändern will, verdirbt es. Wer es besitzen will, verliert es.“

Laozi (6. oder 4. - 3. Jh. v. Chr.), nur legendenhaft fassbarer chinesischer Philosoph, Begründer des Taoismus, (Laotse bedeutet 'der Alte')

1.1 Aufgabenstellung

Eine aktive Steuerung der PDU (sog. „PDU-Controller“) kann durch eine Vielzahl von Ansätzen realisiert werden, die jedoch in die Schnittstellen der PDU selbst, sowie in die übrigen Schnittstellen des Gesamtsystems eingebettet werden müssen. Mit den Arbeiten von Kwiatkowski [17] und Schwarz [27] wurde bereits ein Referenzkonzept für eine PDU ausgearbeitet. Mit der Bachelorthesis von Kwiatkowski wurde der leistungselektronische Teil für dieses Referenzkonzept entwickelt, welches unter anderem ein Erdungskonzept für das gesamte Navigationssystem enthält. In dieser Arbeit werden die verschiedenen Versorgungsleitungen, einschließlich der Sicherungen für die Komponenten des Navigationssystems, definiert. Ferner beinhaltet die PDU elektronische Schalter, die zur An- und Abschaltung der verschiedenen Verbraucher (u. a. Sensoren, Computer, Kommunikations- und Messelektronik) im System verwendet werden sollen. Darüber hinaus wurden in der Arbeit von Kwiatkowski auch leistungselektronische Komponenten wie die DC/DC-Wandler definiert. Die in dieser Arbeit vorgesehenen elektrischen Schnittstellen zur Steuerung der Schalter sind eine wichtige Grundlage für die Erarbeitung eines Konzeptes für eine aktive Steuerung der PDU. Es ist vorgesehen, dass die elektronischen Schalter mit digitalen Spannungssignalen des PDU-Controllers geschaltet werden.

Der PDU-Controller generiert diese digitalen Spannungssignale im Nennbetrieb auf der Grundlage von Befehlen der On-Board-Computer (OBC) des Navigationssystems. Weiterhin soll der PDU-Controller die einzelnen Kanäle der PDU überwachen, wozu er Messwerte aus einer Messschaltung (dem sog. „PDU-Monitor“) anfordert, verarbeitet und den OBCs bereitstellt. Diese Messwerte dienen den OBCs als zusätzliche Stützinformationen zur Bewertung des Betriebszustandes der einzelnen Komponenten. Bei einer Störung soll es möglich sein, einzelne Sensoren und andere Navigationssystemkomponenten auf Befehl der OBCs zu deaktivieren bzw. wieder zu reaktivieren, um auf ein mögliches Fehlverhalten (z. B. Überschreitung des maximalen Nennstromes eines PDU-Kanals durch Kurzschluss) reagieren zu können.

Weiterhin kommt dem PDU-Controller, insbesondere beim Einschalten des Navigationssystems eine besondere Rolle zu: Der Start-Up-Prozess, das heißt die Initialisierung der Navigationssystemkomponenten, mit besonderer Beachtung der Startsequenz der redundanten OBCs, wurde durch Schwarz [27] beschrieben. Da die OBCs die primären Bausteine für die Funktionalität des gesamten Navigationssystems sind, soll der PDU-Controller zur Überwachung des ordnungsgemäßen Starts der OBCs verwendet werden.

Alle diese Funktionen könnten neben der Hauptfunktionalität der PDU durch eine aktive Steuerung der PDU bereitgestellt werden. Aus diesen Überlegungen ergibt sich die Notwendigkeit einer eingehenden Untersuchung möglicher Konzepte für die funktionale und technologische Realisierung eines solchen PDU-Controllers. Bei den Konzepten ist es essenziell, dass sich der PDU-C in das Zuverlässigkeits- und Ausfallsicherheitskonzept des Gesamtsystems einfügt. Das gesamte Navigationssystem soll „*ein-fehlertolerant*“ entworfen werden. Dies bedeutet, dass ein einzelner Fehler nicht zum Ausfall des Gesamtsystems führen darf. Tritt ein Fehler im Gesamtsystem auf, muss es je nach Fehlerart entweder redundante Komponenten (z. B. Sensoren) oder ein Degradationskonzept[1] für die betroffene Komponente geben. Im Fall des PDU-Controllers soll

1 Degradation bedeutet im weitesten Sinne zurückstufen. Ein Degradationskonzept ist in diesem Fall ein Konzept das beschreibt, wie der Funktionsumfang eingeschränkt wird um eine Mindestfunktionalität aufrecht zu erhalten.

ein Fehler im PDU-C selbst nicht zum Ausfall der PDU und damit des Gesamtsystems führen. Daraus folgt eine der Vorgaben an den PDU-C: Ein intrinsisches[2] Degradationskonzept ist zu entwickeln, welches eine kontinuierliche Leistungsversorgung, auch nach Ausfall der Steuerung sicherstellt.

Nach Erarbeitung eines funktionalen Konzeptes (Systementwurf) für einen solchen PDU-Controller soll zudem die technologische Umsetzbarkeit des Entwurfes durch eine Recherche am Markt verfügbarer Komponenten für diesen Systementwurf geprüft werden. Ein wesentlicher Punkt hierbei ist die Beachtung der erwarteten Umgebungsparameter für die angedachten Anwendungen des Navigationssystems. Einflüsse wie Strahlung, Vakuum, schnelle Abfolge von Druckwechseln, mechanischer Schock und starke Temperaturschwankungen stellen besondere Anforderungen dar, die bei der Recherche geeigneter Komponenten berücksichtigt werden müssen.

Die Bearbeitung der Problemstellung soll unter Beachtung der folgenden Annahmen und Bedingungen erfolgen: Der PDU-Controller erhält 20 GPIO-Signale von den OBCs des Navigationssystems. Diese Signale dienen als Schaltanweisungen für die einzelnen PDU-Kanäle. Mit diesen Schaltanweisungen können die OBCs im Betrieb steuern, welche Komponenten des Navigationssystems aktiv oder inaktiv sind. Ferner geht von dem PDU-Controller eine unidirektionale RS-422-Leitung zur Übermittlung von Daten an die OBCs ab. Bei diesen Daten handelt es sich um die Messwerte des PDU-Monitors und, wenn möglich, den Schaltzustand der einzelnen Komponenten. Darüber hinaus soll der PDU-Controller klein und kompakt sein, da das Volumen für das Navigationssystem möglichst gering sein soll. Zum Abschluss ist der eigene Leistungsbedarf des PDU-Controllers so gering wie möglich zu halten, um den gesamten Energiehaushalt des Navigationssystems so wenig wie möglich zu belasten [15].

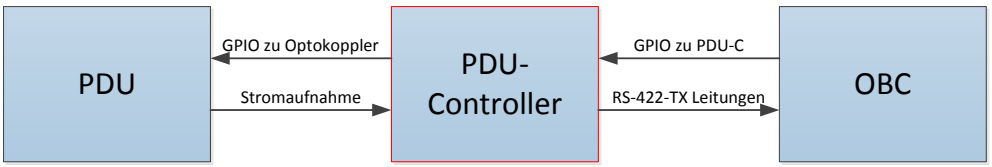


Abbildung 1.1: Schnittstellenübersicht des PDU-C zum Navigationssystems

2 lateinisch intrinsecus „inwendig“, „innerlich“ oder „hineinwärts“, nach der inneren Seite hin

1.2 Ziele der Thesis

Die Bachelorthesis umfasst,

1. die Ausarbeitung, Bewertung und den Vergleich verschiedener Systementwürfe für einen PDU-Controller auf Basis von Konzepten für Redundanz und Fehlertoleranz für Systeme mit komplexen Steuerungsaufgaben aus der Luft- und Raumfahrt, des Automobilbaus sowie der Industrie,
2. die Auswahl eines Systementwurfes anhand einer Aufwands-, Risiko- und Machbarkeitsabschätzung,
3. die Darlegung des mit dem Systementwurf verbundenen intrinsischen Degradationskonzeptes zur Sicherstellung der Leistungsversorgung nach Ausfall des PDU-Controllers und
4. die Spezifikation der für die Realisierung des Systementwurfes notwendigen Schlüsselkomponenten.

Der erste Punkt beleuchtet die theoretischen Grundlagen, die zur Bearbeitung der Aufgabenstellung notwendig sind. Dies umfasst unter anderem Themen wie Redundanz, Diversität sowie die sich ergebenden Konsequenzen hinsichtlich der Zuverlässigkeit bei Serien- und Parallelschaltung von Systemkomponenten. Mittels dieser Informationen ist es möglich, die aus den zuvor genannten Industriebereichen zusammengestellten Systembeispiele nachzuvollziehen und an die gegebene Problemstellung anzupassen. Diese Beispiele werden anschließend auf ihre Vor- und Nachteile im Kontext des geplanten Anwendungsszenarios hin untersucht. Des Weiteren werden einzelne Besonderheiten in den Zuverlässigkeitskonzepten, die Merkmal des betreffenden Industriezweiges sind, herausgearbeitet.

Die unter Punkt 2 genannten Verfahren sind notwendig, um eine fundierte Entscheidung treffen zu können, welches Konzept für das Navigationssystem zweckmäßig ist. Dabei werden mit einer Risikomatrix [16] sowohl die Ausfallwahrscheinlichkeit als auch die Auswirkungen eines Ausfalls bewertet. Nachfolgend werden die einzelnen durchzuführenden Arbeitsschritte zum Umsetzen des Konzeptes abgeschätzt und deren gesamter Aufwand bewertet. Diese beiden Ergebnisse werden abschließend verwendet, um die Machbarkeit des betrachteten Konzeptes zu bewerten.

Der ausgewählte Systementwurf muss auch im Fehlerfall des PDU-Controllers eine Minimalfunktion der PDU gewährleisten. Diese Minimalfunktion muss definiert und deren Erreichen im Fehlerfall oder bei Ausfall des PDU-Controllers (Degradationskonzept), im Hinblick auf den ausgewählten Systementwurf, hinreichend dargelegt werden.

Um eine spätere Weiterführung der Arbeit am PDU-Controller zu ermöglichen, sollen in dieser Thesis konkrete Empfehlungen für wichtige Hardware-Komponenten gegeben werden. Der diesbezügliche Entscheidungsprozess soll hierbei transparent und nachvollziehbar beschrieben werden. Hierfür ist es jedoch zuvor notwendig, die benötigten Spezifikationen für diesen Entscheidungsprozess zu erarbeiten. Dabei kann es sich beispielsweise um Eigenschaften wie die Leistungsaufnahme, die Anschlussmöglichkeiten oder die Verfügbarkeit von Komponenten handeln [15].

2 Theoretische Grundlagen

2.1 Normen und Standards

Zu Beginn dieser Arbeit werden zunächst Normen der unterschiedlichen Industriebereiche zusammengetragen. Dieser Arbeitsschritt soll einen Überblick über die einzuhaltenden Sicherheitsvorgaben geben. Darüber hinaus werden weitere Normen und Standards aus anderen technischen Bereichen untersucht. Dies soll gegebenenfalls eine Erweiterung der möglichen anzuwendenden Planungsmethoden, sowie einen Einblick in die aktuelle Sicherheitstechnik in dem entsprechenden Bereich darstellen.

Raumfahrt

Im Bereich der Raumfahrt finden im europäischen Raum die Normen des Standardisierungsgremiums ECSS (European Cooperation for Space Standardization) Anwendung. Das Ziel der ECSS-Normen ist es, eine gemeinsame Arbeitsgrundlage für Unternehmen im Bereich Luft- und Raumfahrt zu bilden. Dabei hat der Anwender dieser Norm die Möglichkeit sie nicht anzuwenden, sofern er seine Entscheidung begründen kann. Grundsätzlich gilt laut ECSS-S-00C (Description, implementation and general requirements)[6], dass der Auftraggeber vorgibt, welche der Normen anzuwenden sind.

Die folgende Aufzählung ist ein Zitat aus der Norm ECSS-Q-40A Sicherheit[7]:

> Das Design aller Produkte muss so gestaltet werden, dass:
>
> - die Umweltverträglichkeit gewährleistet ist,
> - das Produkt sicher ist, ohne dabei auf externe Dienste angewiesen zu sein,
> - die Fehler, die in Betracht gezogen wurden, das System in eine bestimmte sichere Betriebsart bringen,
> - Gefährdungserkennung, -signalisierung und -sicherung angemessen berücksichtigt sind,
> - Debris[a], Fallout und Aufschlag vermieden werden können,
> - Zugang zum Produkt möglich ist.
>
> *a* Bei Debris handelt es sich weitestgehend um Schutt oder Schrott. Im Zusammenhang mit der Raumfahrt spricht auch von Space Debris. Laut ESA befinden sich zur Zeit (Stand 2005) 600.000 Objekte ohne Funktion mit der Größe 1 cm in der Erdumlaufbahn.

Des Weiteren fordern die zuvor genannten ECSS-Normen, dass die Software mittels bestimmter Methoden und Algorithmen wie zum Beispiel Diversität (Abschnitt 2.3) und dem V-Modell [3] implementiert wird. Ausgenommen von dieser Richtlinie sind Programme, die noch im Betrieb des Systems geändert werden können oder über eine hardwaregestützte Notfunktionalität verfügen. Sollte ein Fehlerfall eintreten, muss das betroffene System den Fehler melden und deutlich kennzeichnen. Parallel zu diesem Vorgang ist es notwendig, dass automatisch ohne äußere Einwirkung, auf ein redundantes System oder einen Störungsmodus umgeschaltet wird. Zu beachten ist bei einem Systemausfall, dass der aufgetretene Fehler keine Auswirkungen auf andere Systemkomponenten hat.

Luftfahrt

Bei der Luftfahrt finden unter anderem die folgenden Normen und Standards zur Entwicklung von sicherheitskritischen Systemen Anwendung [8]:

- EUROCAE ED-80
- RTCA DO-254
- SAE ARP4754
- SAE ARP4761

Bei den Normen für die Luftfahrt sei zunächst erwähnt, dass die amerikanische Organisation RTCA (Radio Technical Commission for Aeronautics) und ihr entsprechendes Pendant, die European Organization for Civil Aviation Equipment oder kurz EUROCAE üblicherweise sehr eng zusammenarbeiten. Einige Dokumente, z.B. die bereits genannten Dokumente ED-80 und DO-254, haben beide den Titel „Design Assurance Guidance for Airborne Electronic Hardware“ und wurden von beiden Organisationen gemeinsam entwickelt [8].

Tabelle 2.1: Festlegung von Design Assurance Levels (DAL) [14]

Fehlerklassifizierung	DAL	Ausfallwahrscheinlichkeit pro Flugstunde	Häufigkeit des Auftretens
Katastrophal	Level A	$< 10^{-9}$	extrem unwahrscheinlich
Gefährlich	Level B	$< 10^{-7}$	äußerst gering
Bedeutend	Level C	$< 10^{-5}$	gering
Gering	Level D	$< 10^{-3}$	vereinzelt
Keine Auswirkungen	Level E	-	gelegentlich

Bei den Dokumenten SAE ARP-4754 „Guidelines For Development Of Civil Aircraft and Systems“ und SAE ARP-4761 „Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment“ handelt es sich um Abläufe bzw. Methoden zur Sicherheitsbewertung. Dabei wird in diesen beiden Dokumenten auf den Planungsablauf in

3 Das V-Modell ist eine Planungsmethode in der Softwareentwicklung. Es werden dort mehrere Schritte beschrieben ein Projekt zu Planen dies beinhaltet unter anderem auch die Qualitätssicherung

einem Projekt bzw. in einem Teilsystem eingegangen. Der Prozess beginnt mit den Anforderungen, die an ein System gestellt werden. Dabei kann es sich sowohl um Umgebungsparameter, als auch den Systemfunktionsumfang handeln. Aus den gegebenen Rahmenbedingungen erfolgen somit indirekt die nötigen Vorgaben für die Hard- und Softwarearchitektur. Parallel zu diesem Prozess erfolgt eine Sicherheitsanalyse, in der das zu erstellende System bzw. dessen möglicher Ausfall bewertet wird. Ähnlich, wie die zuvor genannten Normen ED-80 und DO-254 wird auch in diesen Normen die DAL-Einstufung verwendet 2.1.
Die in diesem Abschnitt genannten und in Abbildung 2.1 gezeigten Standards haben alle ein ähnliches Vorgehen:

1. Aufgabenbeschreibung des Systems
2. Bestimmen der Sicherheitsklasse, anhand der Systemanforderungen
3. Entwicklung von Vorschlägen zu verschiedenen Verfahren zur Planung eines Systems ohne Ausfälle und undefinierten Zuständen

Bei den im dritten Punkt genannten Verfahren, unterscheiden sich jedoch die einzelnen Normen geringfügig voneinander. Jedoch soll bei allen durch eine strukturierte und ausführliche Projektplanung dafür gesorgt werden, dass das zu planende System nicht ausfällt oder bei einem Fehlerfall keine Schäden entstehen. Hierbei gilt als Grundsatz, Personenschäden sind auf jeden Fall zu vermeiden.
Um diese Vorgaben zu erreichen, werden in den Standards unterschiedliche Verfahren und Werkzeuge vorgegeben. Diese sind unter anderem das V-Model, FMEA (Failure Mode and Effects Analysis), Fehlerbaumanalysen und das Fischgrätendiagramm.

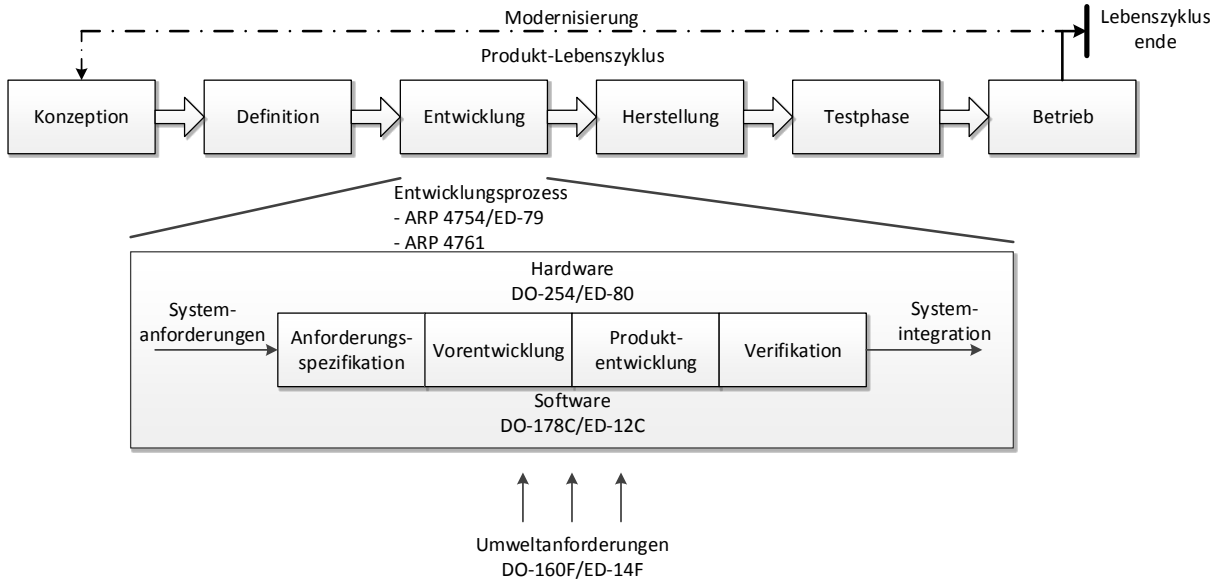


Abbildung 2.1: Prozess der Systementwicklung mit relevanten Standards. (entspricht der Abbildung 3.5 in dem Buch von Flühr [8])

Automobilbereich

Die im Automobilbereich anzuwendende Norm ist die ISO 26262. Genau wie in den vorangegangenen Abschnitten handelt es sich bei diesem Standard primär um eine Beschreibung organisatorischer Vorgänge zur Qualitätssicherung und des Projektmanagements. Sie definiert zur Einstufung folgende (Tabelle 2.2) ASIL (Automotive Safety Integrity Level) Bereiche [10]. In anderen Prozessindustriezweigen wird, anstelle des ASIL, auch die Klassifizierung nach SIL verwendet.

Tabelle 2.2: Ausfall-Wahrscheinlichkeitsgrenzwerte aus der ISO 26262

ASIL	**Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde**
A	$< 10^{-5}$
B	$< 10^{-6}$
C	$< 10^{-7}$
D	$< 10^{-8}$

Das nach einer Sicherheitsanalyse bestimmte Level hat Auswirkung auf das weitere Vorgehen im Projekt. Bei der Auswahl von Level D sind die auszuführenden Maßnahmen umfangreicher, als bei Level A. Die unterschiedlichen Level beinhalten zum einen festgeschriebene, als auch empfohlene Vorgänge zur Projektplanung und Qualitätssicherung. Es bleibt dem Anwender bei der Planung überlassen, welche Vorgänge er beim Tailoring[4] aussparen oder in die Planung mit einbeziehen möchte. Wichtig ist dabei jedoch, dass die zuvor angestrebte Ausfallwahrscheinlichkeit erreicht wird.

Prozessindustrie

Neben Vorgaben des Gesetzgebers findet im Bereich der Industrieanlagen ein hierarchisches System von Normen Anwendung. Man spricht dabei von A, B, C-Normen. A-Normen wie die ISO 12100-1 beinhalten primär Grundbegriffe und allgemeine Gestaltungsgrundsätze. Für diese Ausarbeitung von besonderer Bedeutung ist die Norm DIN EN ISO 14121-1, diese beinhaltet unter anderem die Durchführung einer Risikobeurteilung.
B-Normen, wie beispielsweise die DIN EN 999, beschreiben: „Sicherheit von Maschinen - Anordnung von Schutzeinrichtungen im Hinblick auf Annäherungsgeschwindigkeiten von Körperteilen“. Da die darin behandelten berührungslosen Schutzeinrichtungen, wie z.B. Lichtschranken, nicht auf bestimmte Arten von Maschinen beschränkt sind, ist dort beschrieben, wie eine Anlage beim Auslösen dieser Einrichtung zu reagieren hat.
C-Normen enthalten sehr präzise Angaben über eine bestimmte Maschinengruppe. Zum Beispiel beinhaltet die Norm DIN EN 422 die grundsätzliche Beschaffenheit von Kunststoff- und Gummimaschinen.

4 Unter Tailoring versteht man die Anpassung eines festgelegten Verfahrens oder einer Methoden an den benötigten Bedarf.

Von hoher Bedeutung in allen Industriebereichen ist die IEC (EN) 61508. Sie stellt eine Grundlage für viele unterschiedliche Standards dar. Normen und Standards wie die ISO 26262, die IEC 61511 oder die DO-178B sind eine branchenspezifische Umsetzung der IEC 61508.[24]

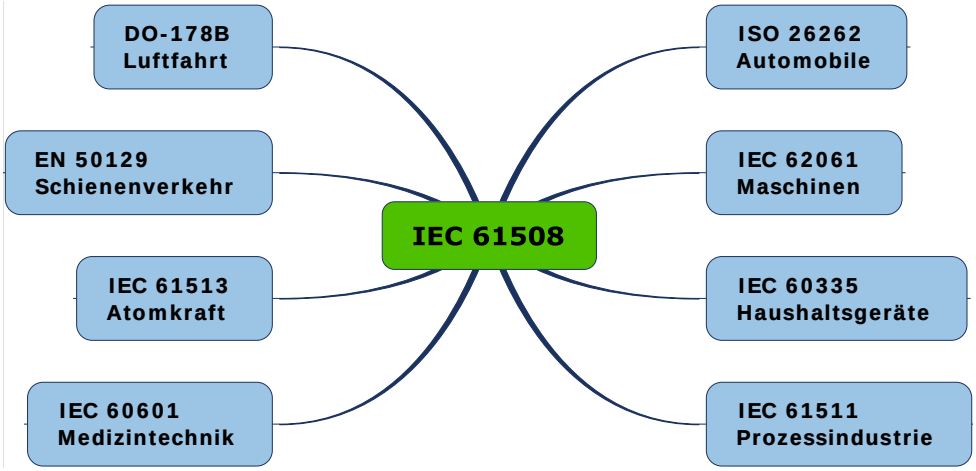


Abbildung 2.2: Standards, die auf der IEC 61508 basieren (Grafik basiert auf Abbildung 5 in [24])

Die Norm IEC 61508 beschäftigt sich mit der Bewertung von Risiken. Die IEC 61508 definiert dabei vier unterschiedliche SIL-Sicherheitsstufen. Im Gegensatz zum KFZ-Bereich (Abschnitt 2.1), wird hierbei jedoch zwischen Low Demand- und High Demand-Systemen unterschieden. Low Demand Systeme haben geringere Anforderungen an die Sicherheitssysteme. Dabei darf das Sicherheitssystem nur einmal im Jahr aktiv werden. High Demand-Systeme haben hohe Anforderungen an das Sicherheitssystem. Sie arbeiten kontinuierlich mit und gewährleisten somit eine sehr hohe Sicherheit.

Tabelle 2.3: Ausfallgrenzwerte für eine Sicherheitsfunktion, die in der Betriebsart mit hoher oder kontinuierlicher Anforderungsrate betrieben wird (High Demand).[2].

SIL	PFH (pro Stunde)	Max. akzeptierter Ausfall des SIL
SIL 1	$\geq 10^{-6}$ bis $< 10^{-5}$	ein gefährlicher Ausfall in 100.000 Stunden
SIL 2	$\geq 10^{-7}$ bis $< 10^{-6}$	ein gefährlicher Ausfall in 1.000.000 Stunden
SIL 3	$\geq 10^{-8}$ bis $< 10^{-7}$	ein gefährlicher Ausfall in 10.000.000 Stunden
SIL 4	$\geq 10^{-9}$ bis $< 10^{-8}$	ein gefährlicher Ausfall in 100.000.000 Stunden

Eine weitere übliche Klassifizierung in der Industrie ist die DIN V 19250 „Leittechnik - Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen“. In dieser Norm werden einzelne AK (Anforderungsklassen) definiert. Einzelne Geräte werden bei der Entwicklung diesen Anforderungsklassen zugewiesen. Diese Norm hat den Nachteil, dass immer nur einzelne Komponenten betrachtet werden. Eine Klassifizierung mit einer Anforderungsklasse trifft also keine Aussage über die gesamte Systemsicherheit. Ferner wurde, die deutsche Norm, DIN V 19250 inzwischen im zuge einer europäischen Vereinheitlichung durch die Nachfolge Norm EN 61508 abgelöst. Demzufolge wurde die DIN V 19250 zurückgezogen. Da Anforderungsklassen in der Praxis weit verbreitet sind, werden sie zusätzlich in Tabelle 2.3 aufgeführt.

Tabelle 2.4: Vergleich von AKs (DIN V 19250) und SIL (IEC 61508)[2].

Anforderungsklasse nach DIN V 19250	**Safety Integrity Level**
AK 1	nicht definiert
AK 2 AK 3	SIL 1
AK 4	SIL 2
AK 5 AK 6	SIL 3
AK 7 AK 8	SIL 4

Eine weitere Industrienorm ist die Maschinenrichtlinie (CE-Kennzeichnung). Mit der Kennzeichnung eines Gerätes mit dem CE-Zeichen versichert der Hersteller, dass sein Produkt den Ansprüchen der Maschinenrichtlinie [20] genügt. Dabei ist die CE-Kennzeichnung kein Siegel, dass durch eine Institution vergeben wird. Daraus folgt, dass es sich beim der CE-Kennzeichnung um ein Verwaltungszeichen handelt. Die Maschinenrichtlinie hat keine rechtliche Bewandtnis, da sie wie alle europäischen Richtlinien zunächst in das nationale Recht überführt werden müssen. Diese Überführung geschieht in Deutschland in dem Produktsicherheitsgesetz (ProdSG), welches explizit auf die Maschinenrichtlinie verweist. Unter Punkt 1.2.1 „Sicherheit und Zuverlässigkeit von Steuerungen“ in der Maschinenrichtlinie ist beschrieben, welche Sicherheitsanforderungen ein Gerät haben muss, jedoch nicht wie dies umzusetzen sind. Somit eignet sich die Maschinenrichtlinie nur bedingt dafür bei der Entwicklung des PDU-C berücksichtigt zu werden.

Eine Risikobeurteilung in der Industrie erfolgt fast analog zu der Risikobeurteilung im Automobilbereich im Abschnitt 2.1. Hier wird ebenfalls eine Risikobeurteilung mittels Risikobaum vorgenommen.

Zwischenfazit

Die beschriebenen Normen in diesem Abschnitt haben unabhängig voneinander alle einen ähnlichen Ablauf (Abbildung 2.3 [13]). Dieser Ablauf ist in fast allen, in dieser Arbeit beschrieben Normen und Standards enthalten. Da es sich um eine allgemeine Norm handelt wird in ihr von E/E/PE-Systemen (Funktionale Sicherheit von elektrischen / elektronischen / programmierbaren elektronischen Sicherheitssystemen) gesprochen. Diese Ähnlichkeit im Ablauf lässt sich damit begründen, dass bei der Entwicklung der IEC 61508 Anleihen aus den früher vorhandenen Normen und Standards der Luft- und Raumfahrt genommen wurden. Abschließend lässt sich zu diesem Abschnitt sagen, dass die komplette Konzeptentwicklung nach einer der zuvor genannten Normen nicht möglich bzw. nicht notwendig ist. Dies hat folgende Gründe:

- Der Arbeitsumfang einer Bachelorthesis reicht für eine komplette Konzeptplanung, die nach einer der zuvor genannten Normen durchzuführen.
- Nach Rücksprache mit dem Subsystemverantwortlichen, des Navigationssystemes, in der DLR Abteilung GNC darf ein Personenschaden nur mit einer Wahrscheinlichkeit von $< 10^{-9}$ Eintreten. Da es sich bei SHEFEX III um eine Forschungs- und Versuchsmission handelt, wird darauf verzichtet weitere Anforderungen an die Zuverlässigkeit, der einzelnen Baugruppen zu stellen. Überdies hinaus wird trotzdem versucht den PDU-C so Fehlertolerant wie möglich zu gestalten. Da Navigationssystem so ausgelegt sein soll, dass es zukünftig für andere Missionen verwendbar ist. Da das Navigationssystem folglich keiner direkten Sicherheitseinstufung unterliegt, unterliegt auch das Navigationssubsystem, der PDU-C keiner direkten Vorgabe.
- Da es bei dieser Thesis primär um das Erstellen und Bewerten von Konzepten geht, ist es nicht notwendig, eine komplette Normenumsetzung vorzunehmen. Bereiche wie die Luft- und Raumfahrt schreiben vor, dass die Umsetzung eines Konzeptes umfangreich getestet werden muss. Diese Tests sind notwendig, um sicher zustellen, dass ein System auch den zuvor definierten Sicherheitsanforderungen genügt. Da es aber nicht Aufgabe dieser Thesis ist ein PDU-C zu erstellen und zu testen, ist es folglich in dieser Thesis nicht möglich allen Anforderungen gerecht zu werden.
- Da es sich bei SHEFEX III um einen Forschungsprojekt handelt, das eine kurze Missionsdauer hat und nach dem Prinzip Design to Cost[5] geplant wird, wurde von der Projektleitung entschieden auf eine exakte Einhaltung der ECSS Normen zu verzichten. Die ECSS Normen kommen jedoch weiterhin getailort zur Anwendung. Darüber hinaus wird ein Missions Scenario gewählt, bei dem es Aufgrund der Flugrute nicht zu einer Gefährdung von Personen kommen kann.

Dessen ungeachtet werden Analysen aus diesen Normen verwendet, um die Entwicklung der Konzepte durchgeführen:

- **Machbarkeitsbewertung mit einem Morphologischen Kasten nach VDI 2225 -** bei einem morphologischen Kasten handelt es sich um Werkzeug zum auswerten mehrerer entscheidungs-Parameter.

5 Design to Cost bedeutet, dass zu Beginn eines Projektes eine Finanzplanung vorgenommen wird. Mit diesem Geld muss das Projekt umgesetzt werden, es gibt keine nachträglichen Finanzierungsänderungen.

- **FMEA (Failure Mode and Effects Analysis) -** Die FMEA wird eingesetzt, um mögliche Fehlerquellen hinsichtlich ihrer Bedeutung, Auswirkung und Eintrittswahrscheinlichkeit zu bewerten.
- **Ursache-Wirkungs-Diagramm -** Das Ursache-Wirkungs-Diagramm geht der FMEA voraus und wird als Hilfsmittel zum sammeln von Fehlerursachen verwendet.
- **Risikoanalyse -** Die Risikoanalyse ist eine weitere Möglichkeit Fehlerquellen zu bewerten. Gegenüber der FMEA bezieht sich die Risikoanalyse aber meistens auf organisatorische Probleme.

Diese Projektplanungsmethoden und Qualitätsmanagment sind ein Bestandteil der in diesem Abschnitt beschriebenen Normen. Ferner stellen diese Methoden einen guten Kompromiss zwischen einem akzeptablen Arbeitsaufwand für diese Bachelorthesis und einer sicheren Projektplanung dar.

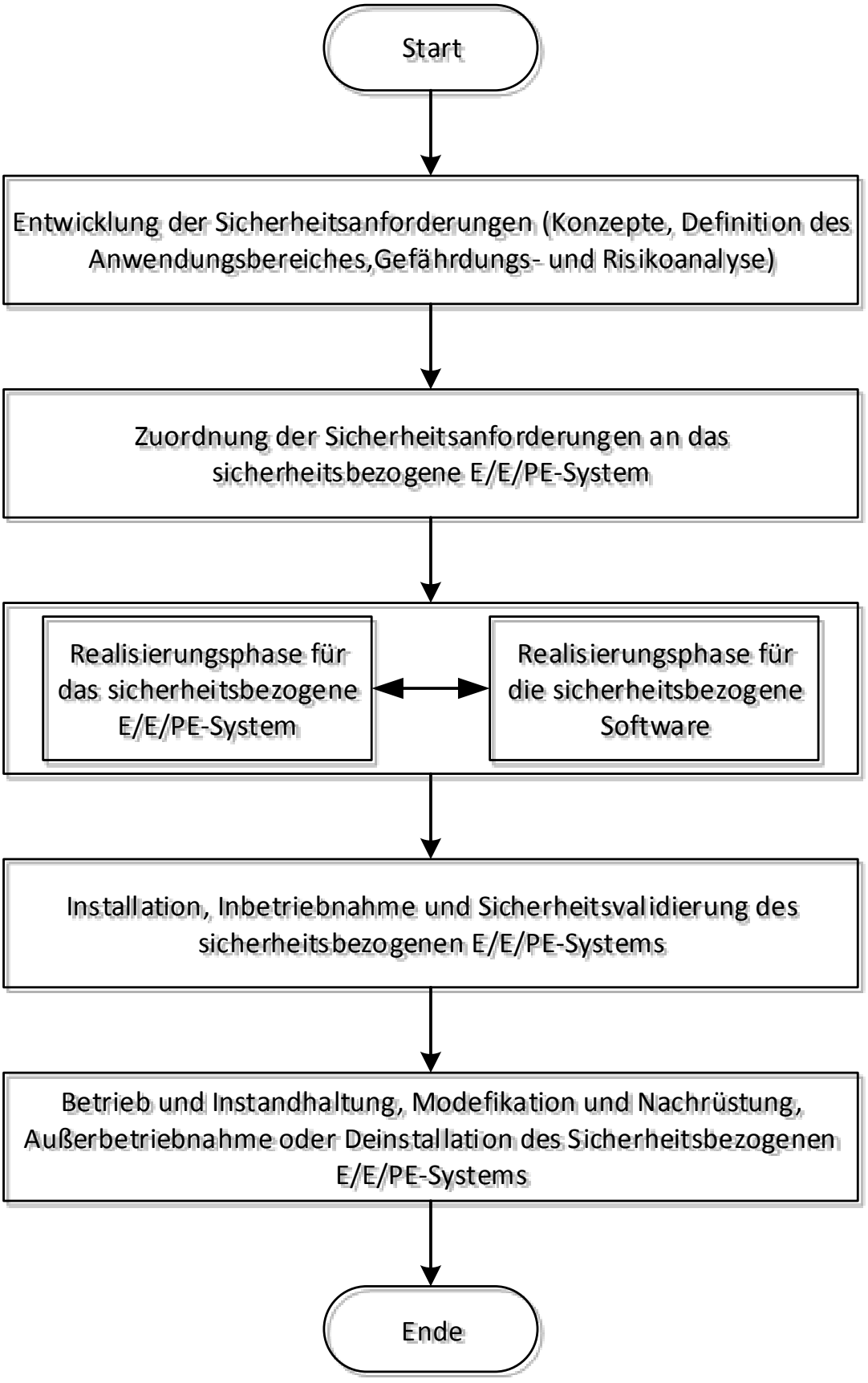


Abbildung 2.3: Vereinfachter struktureller Ablauf des Standards der IEC 61508

2.2 Ausfallwahrscheinlichkeit

Dieses Kapitel bildet die Grundlage für die spätere Konzeptionierung des PDU-Controllers (Kapitel 3). Ziel ist es, die theoretischen Grundlagen für das spätere Systemdesign herauszuarbeiten.

2.2.1 Ausfallrate

In der Praxis hat es sich etabliert, die Zuverlässigkeit eines Systems mit der Ausfallrate λ anzugeben. Die Ausfallrate λ ist der Parameter einer statistischen Lebensdauerverteilung und gibt die Anzahl von Ausfällen je Zeiteinheit an. Als Einheit wird dabei üblicherweise die Einheit FIT (Failure in Time) verwendet, wobei

$$1\,\mathrm{FIT} = 1 \cdot 10^{-9}\,\frac{1}{\mathrm{h}}. \tag{2.1}$$

Dem zufolge ereignet sich alle 10^9 h ein Ausfall, dies entspricht ca. 114 000 Jahren. Eine übliche Quelle für FIT-Werte ist das Militärhandbuch MIL-HDBK-217F und die Siemens-Norm SN 29500. Es muss jedoch darauf hingewiesen werden, dass die FIT-Werte für Bauteile, je nach Quelle, sehr stark schwanken können und stark von physikalischen Einflüssen abhängig sind. Die Lebensdauer eines Bauteil kann auch wesentlich kürzer sein. Dabei folgt die Verteilung der Ausfälle mehrerer Bauteile eines Typs einer Badewannenkurve (Darstellung 2.4). Diese teilt sich in die folgenden drei Teile auf.

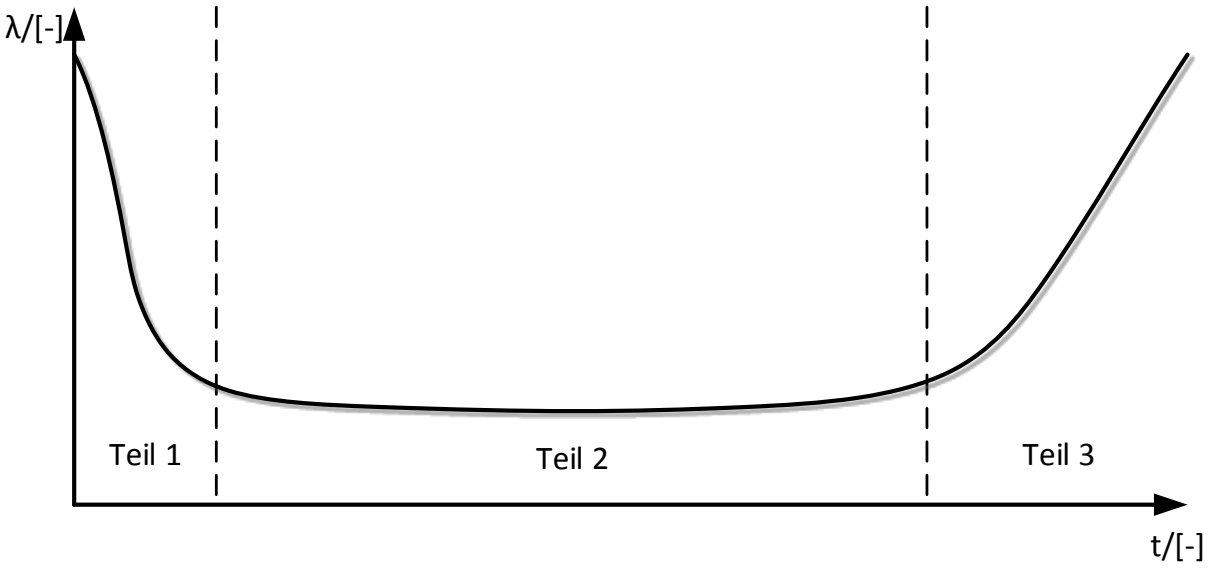


Abbildung 2.4: Badewannenkurve zur Beschreibung des zeitlichen Verlaufs der Ausfallrate λ

- **Teil 1 Frühphase**
  In dieser Phase finden Frühausfälle statt. Diese können durch Produktionsfehler oder schlechte Verarbeitung in der Herstellung entstehen.

- **Teil 2 Nutzungphase**
  In dieser Phase erreicht $\lambda(t)$ sein Minimum und ist weitestgehend konstant.
- **Teil 3 Verschleißphase**
  Zum Ende der Lebensdauer eines Bauteils steigt $\lambda(t)$ wieder an. Zum Ende der Lebensdauer eines Bauteils treten Ausfälle, aufgrund von Bauteilalterung, wieder verstärkt auf.

2.2.2 Zuverlässigkeit

Die Zuverlässigkeit $R(t)$ ist die Wahrscheinlichkeit, dass eine betrachtete Komponente zum Zeitpunkt t funktionsfähig ist. Tritt der Fall ein, dass der Wert t sehr klein ist, ist somit die Wahrscheinlichkeit (T) das eine Komponente zu diesem Zeitpunkt funktionsfähig ist sehr groß (Wert 1).

$$R(t) = e^{-\lambda \cdot t} \tag{2.2}$$

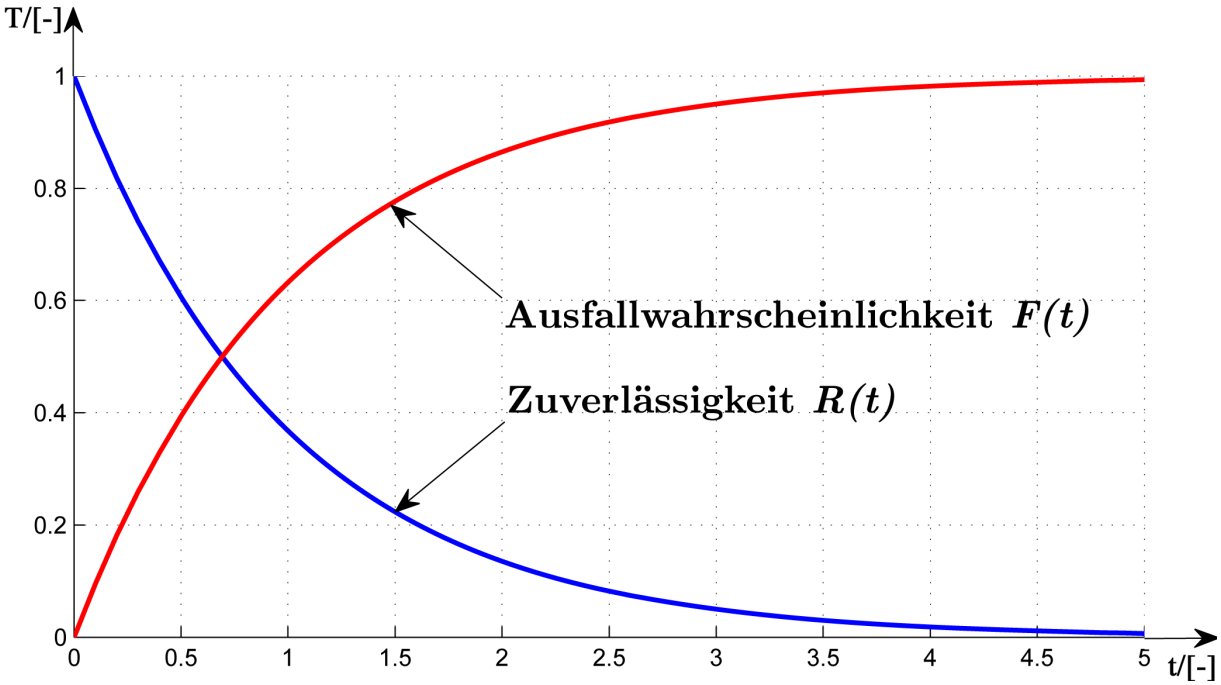


Abbildung 2.5: Zeitlicher Verlauf der Zuverlässigkeitsfunktion $R(t)$ und der Ausfallwahrscheinlichkeit $F(t)$ eines Systems bei konstanter Ausfallrate

2.2.3 Ausfallwahrscheinlichkeit

Bildet man das Komplement der Zuverlässigkeitsfunktion, erhält man die Ausfallwahrscheinlichkeit $F(t)$. Die Ausfallwahrscheinlichkeit $F(t)$ ist die Wahrscheinlichkeit, dass eine betrachtete Komponente zum Zeitpunkt t nicht funktionsfähig ist.

$$F(t) = 1 - R(t) \tag{2.3}$$

2.2.4 Zuverlässigkeit von Systemen

In mechanischen Anwendungsgebieten ist es weit verbreitet, Sicherheitsfaktoren in die Berechnung eines Systems mit einfließen zu lassen. Ferner ist es gängige Praxis ein System so zu gestalten, dass beim Versagen eines Bauteils, ein anderes die komplette Funktionalität weiterhin gewährleistet. So ist es zum Beispiel weitestgehend ausgeschlossen, dass ein Fahrstuhl abstürzt, da zum Einen die Seile mindestens mit einem Sicherheitsfaktor von 12 beaufschlagt werden und zum Anderen immer mehr als ein Seil (Redundanz) im Gesamtsystem Fahrstuhl verwendet wird. Das in dem oberen Beispiel erläuterte verwenden mehrerer gleicher Komponenten, wird Redundanz genannt. Diese Technik wird häufig verwendet wenn technische Systeme Fehlertolerant entworfen werden müssen. Grundsätzlich werden folgende Redundanz-arten unterschieden:

- **Heiße Redundanz:** Das redundante Element wird von Beginn an der gleichen Belastung im System ausgesetzt.
- **Warme Redundanz:** Das redundante Element arbeitet mit, wird aber nicht voll belastet.
- **Kalte Redundanz:** Das redundante Element ist bis zum Zeitpunkt des Ausfalls unbelastet und wird erst im Fehlerfall zugeschaltet.

Beim Entwurf von elektronischen Schaltungen ist diese Vorgehensweise noch nicht überall verbreitet. Ausnahmen bilden im diesem Bereich die Luft- und Raumfahrt sowie Sicherheitssysteme im KFZ-Bereich. Ein weiteres Problem ist ferner die Nichtbeachtung der Umgebungsparameter, was dazu führt, dass beispielsweise die Betriebstemperaturen vernachlässigt werden. Dies führt dazu, dass Bauteile nicht mehr in ihres optimalen Arbeitsbereiches sind und deshalb durchbrennen oder eine schnellere Alterung dieser Bauteile stattfindet.

Seriensysteme

Üblicherweise bestehen Systeme aus mehreren einzelnen Komponenten. Im Betrieb muss jedes Bestandteil seine ihm zugewiesene Funktion erfüllen. Sollte eine Komponente ausfallen, führt dies üblicherweise dazu, dass das gesamte System ausfällt. Bei solch einer Architektur spricht man von einer Serienstruktur.

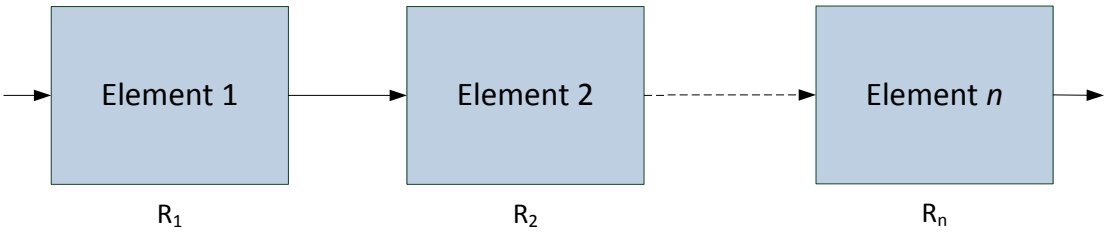


Abbildung 2.6: Serienschaltung von Komponenten

Um nun die Zuverlässigkeit zu bestimmen, muss das Produkt der einzelnen Komponenten $R(t)$ zu bilden.

$$\begin{aligned} R_{SysS}(t) &= R_1(t) \cdot R_2(t) \cdot \ldots \cdot R_n(t) \\ &= \prod_{i}^{n} R_i(t) \end{aligned} \tag{2.4}$$

MTBF Mittlere Brauchbarkeitsdauer

Die mittlere Brauchbarkeitsdauer (MTBF Mittlere Brauchbarkeitsdauer) ist die mittlere Zeit zwischen zwei Ausfällen und berechnet sich wie folgt [33]:

$$MTBF = \frac{1}{\lambda} \cdot \sum_{i=k}^{n} \frac{1}{i} \tag{2.5}$$

k-aus-n-Systeme

k-aus-n-Systeme sind Systeme aus n identischen, von einander unabhängigen Komponente, von denen mindestens k Komponenten funktionieren müssen, damit das Gesamtsystem funktioniert [4]. Die Zuverlässigkeit einer solchen k aus n Kombination, aus gleichen Komponenten und somit aus der gleichen Komponentenzuverlässigkeit R kann mit der Binomialverteilung[6] berechnet werden[33].

$$R_{ges} = \sum_{i=k}^{n} \left(\begin{array}{c} n \\ i \end{array} \right) \cdot R^i \cdot (1-R)^{n-i} \tag{2.6}$$

6 Die Binomialverteilung bezeichnet eine Kurve, die beim Bernoulli-Experiment entstanden ist. Sie ist eine wichtige diskrete Wahrscheinlichkeitsverteilung. Die Binomialverteilung beschreibt den wahrscheinlichen Ausgang einer bestimmten Anzahl von gleichen Versuchen. Diese Versuche haben dabei nur einen positiven oder negativen Ausgang.

In der bereits zitierten Literatur wird hierfür häufig eine *koon* Schreibweise verwendet. Eine 2oo4 Systembeschreibung ist ein System bei dem 2 von 4 Komponenten für den Betrieb funktionsfähig sein müssen. Diese Art der Systembeschreibung hat den Vorteil, dass schnell und einfach ein Überblick über die Systemarchitektur gegeben werden kann.

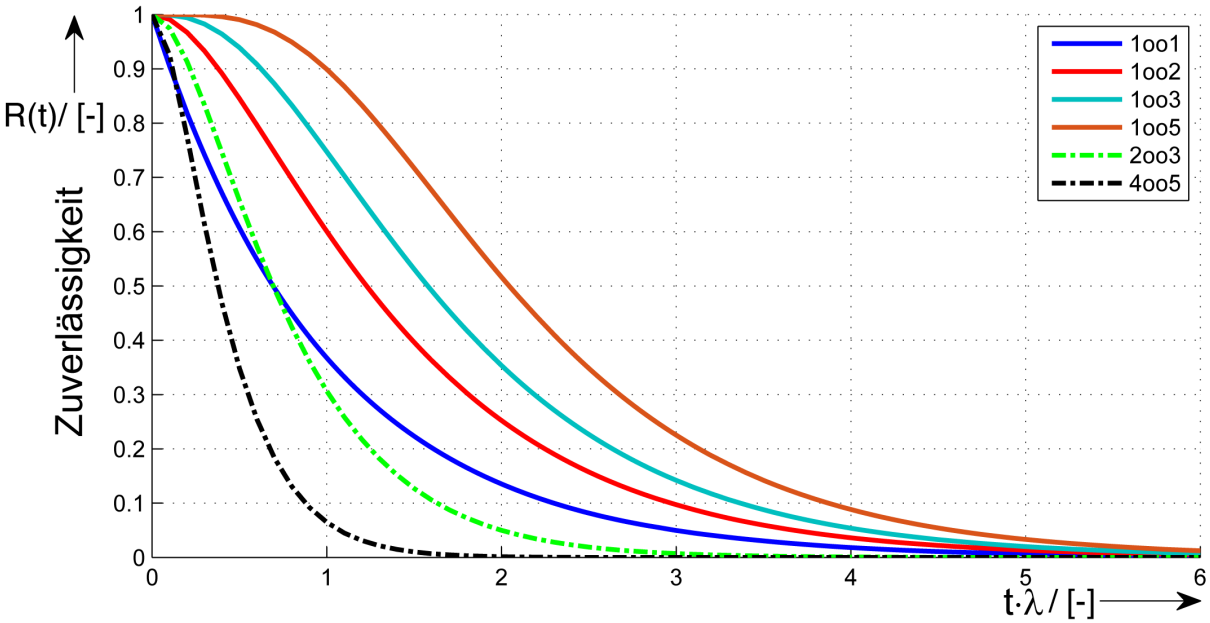


Abbildung 2.7: Zuverlässigkeit unterschiedlicher k aus n Systeme in Abhängigkeit von der Zeit

Auf der Abbildung 2.7 ist zu erkennen, dass eine reine Erhöhung der identischen Systempfade zu einer Verbesserung der Zuverlässigkeit führt. Jedoch ist auch zu erkennen, dass eine 1oo2 Kombination zuverlässiger als eine 2oo3 Variante ist. Dies fällt auf, da die 2oo3 Kombination häufig Verwendung findet wenn Daten miteinander verglichen werden. Daraus lässt sich schlussfolgern, dass bei einer einfachen theoretischen Betrachtung, wie in diesem Fall, die Erhöhung der Datensicherheit durch ein 2oo3 System die physikalische Gesamtzuverlässigkeit senkt, im Vergleich zu einem 1oo2 System.

Beim Erstellen von zuverlässigen Systemen gibt es keine richtige oder falsche Lösung. Wichtig bei einem Lösungsansatz sind die zugrunde liegenden Rahmenbedingungen. Platz, Kosten, Gewicht und technische Umsetzbarkeit sind häufig limitierende Elemente bei der Systemsynthese. Ist es zum Beispiel notwendig, eine Energieversorgung mit DC/DC-Wandlern sicher in heißer Redundanz zu erstellen, wird dies Auswirkungen auf die Eigenschaften der Wandler haben und somit auch auf die Größe, Gewicht und den Wirkungsgrad.
Aus diesem Grund sind in der Praxis diverse Kombinationen aus Serien-und Parallel-Konfigurationen gängig. Häufig hängen solche Designentscheidungen auch von den verwendeten Bauteilen an sich ab. So besitzt ein Schalter im KFZ-Bereich einen FIT-Wert von ca. 1500 [25], was im Vergleich zu Metallfilmwiderstand mit einem Wert 2 relativ hoch ist. Die Konsequenz aus diesem Verhältnis ist, dass man sofern möglich, den Schalter fehlertolerant auslegen wird, den Widerstand im direkten Vergleich jedoch nicht.

2.3 Diversität

Der Ansatz der Diversiät[18] bietet die Möglichkeit, die Auswirkung durch bauartbedingte Fehler und fehlerhaftem Design zu verringern. Grundsätzlich wird bei diesem Verfahren ein mindestens doppelt parallel redundantes System entworfen. Allerdings werden bewusst unterschiedliche Realisierungen gewählt und keine baugleichen Komponenten verwendet. Hinter dem Verfahren der Diversität steht die Idee, dass es für eine vorhandene Aufgabe mehrere mögliche Lösungen gibt. Der Umfang der Diversität hängt dabei vom Entwickler ab. Im Fall einer Mikrocontrollerschaltung kann das bedeuten, dass zwei unterschiedliche Controller verwendet werden. Möglich ist aber auch, dass die Software von zwei unterschiedlichen Personen in unterschiedlichen Programmiersprachen geschrieben wird.

2.4 Praktische Anwendungsfälle der theoretischen Grundlagen

Raumfahrt

Überall dort wo ein Systemausfall zu einem missionskritischen Zustand führt oder sogar Menschenleben in Gefahr sind, wird in der Raumfahrt bei elektronischen Systemen häufig eine 3oo4 Anordnung verbaut. Diese Einheiten werden synchronisiert und führen parallel identische Vorgänge aus. Sollte eine Einheit ausfallen, sind die verbliebenen Einheiten mittels einer Majoritätsentscheidung in der Lage, die Funktionsfähigkeit des Systems zu gewährleisten. Sollte dennoch ein zweiter Fehler auftreten, was sehr unwahrscheinlich ist, ist ein 2oo4-System weiterhin funktionsfähig. Diese Systemkonfiguration kam z.B. bei den Start-und Landesystemen der Space Shuttles zum Einsatz. Auch die geplante Raumfähre Hermes der ESA sollte mit solchen Systemen ausgestattet. Das 2oo4-System hat jedoch einen Nachteil, im Fall von 4 redundanten Computern ist der Energieverbrauch sehr hoch. Aus diesem Grund werden sie beispielsweise, wenn das Space Shuttle die Systeme nicht benötigt, deaktiviert [12].

Luftfahrt

In der Luftfahrt sei zunächst als praktisches Beispiel ein Fly-by-Wire[7] System genannt. Dieses muss mit einer Ausfallwahrscheinlichkeit von 10^{-9} absolut sicher sein und nie komplett ausfallen. Dabei sind die elektronischen Komponenten, die Daten erfassen, verarbeiten und übertragen redundant ausgelegt. Erwähnenswert ist in diesem Zusammenhang, dass die Software, die auf den Computern zum Einsatz kommt unterschiedlich gestaltet werden muss und somit einem Diversitätsansatz (Abschnitt 2.3) folgt [21]. Dieses Vorgehen ist notwendig, da eine reine Hardwarevervielfachung nicht vor Softwarefehlern schützt.

Automobilbereich

Ein typisches Beispiel für Redundanz im Automobilbereich ist das Bremssystem. Grundsätzlich sind zwei voneinander getrennte Systeme vorhanden. Jedes System steuert hierbei 2 Räder. Sollte eines ausfallen, ist das zweite immer noch in der Lage das Auto zum Stehen zubringen. Man kann also von einem 1oo2-System sprechen. Die gleiche Systemkonfiguration (1oo2) gibt es auch bei Motorrädern. Vorder- und Hinterradbremse sind hier vollkommen getrennte Systeme. Moderne Systeme im Auto sind dagegen nicht mehr so einfach zu klassifizieren. Aktuelle Ansätze betrachten jede Komponente einzeln. Das bedeutet Systeme sind nicht mehr komplett parallel oder seriell sondern gemischt. Abbildung 2.8 zeigt ein konventionelles und ein modernes Redundanzkonzept. Bei beiden Konzepten handelt es sich um die Sensorik von elektronischen Lenkungen im Auto. Die rechte Seite zeigt eine elektronisch unterstützte mechanische Lenkung, die linke Seite zeigt ein Konzept für eine vollelektrische Steer-by-Wire Lenkung.

7 *X*-by-Wire bezeichnet den Ersatz von manuell gesteuerten mechanischen Systemen durch elektrisch miteinander verbundene Bedienelemente und Aktoren.

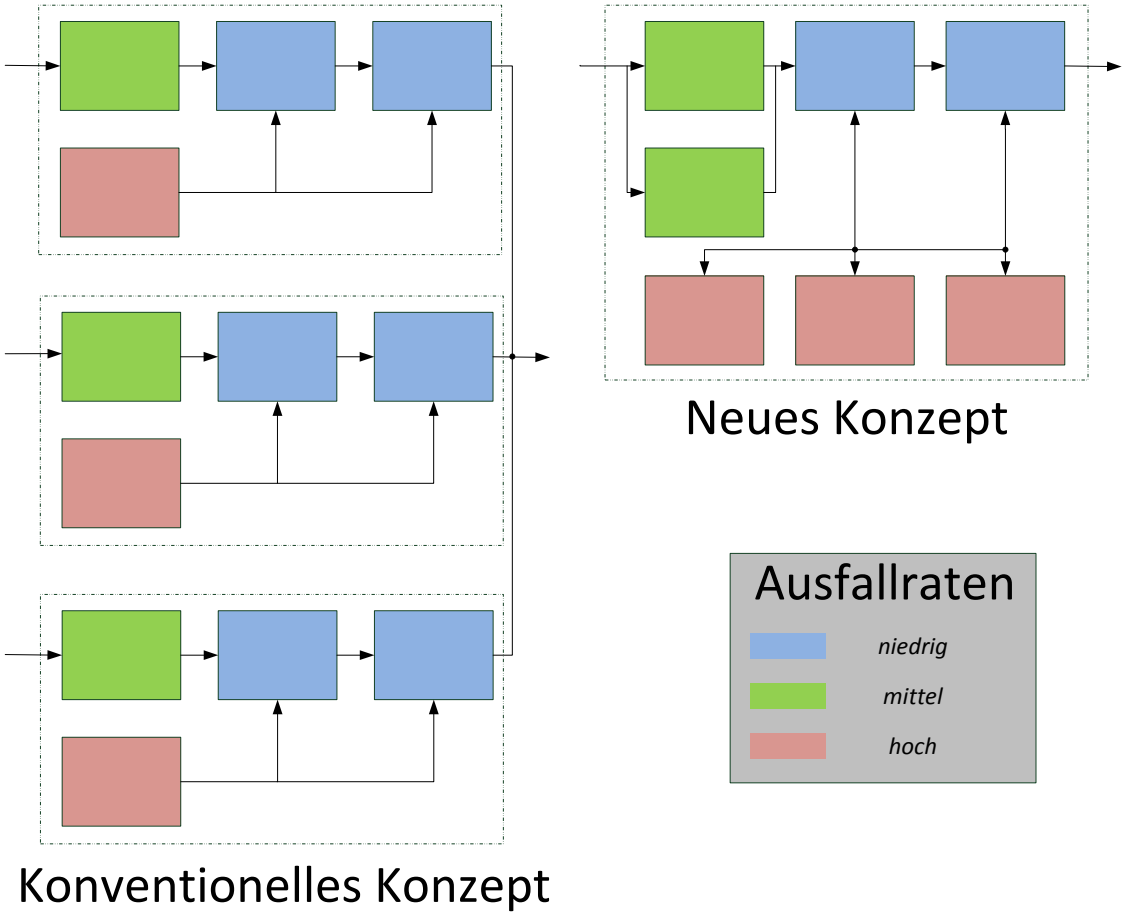


Abbildung 2.8: Vergleich zwischen konventioneller und moderner Redundanz

Industrie

Häufig werden in der Industrie in sicherheitsrelevanten Systemen Stellantriebe verwendet. Aus diesem Grund ist ein solcher Stellantrieb ein gutes Beispiel, um zu verdeutlichen, wie aus einem Stellantrieb ohne SIL-Klassifizierung in der Praxis ein sicheres System gemacht wird. Eine Möglichkeit ist, einem bereits vorhandenem Antrieb eine zusätzliche Sicherheitsplatine hinzuzufügen. Kommt es nun zu einer Störung, wird die vorhandene Logik überbrückt und das System wird mit der sehr einfach ausgelegten Logik der SIL-Platine in einen definierten sicheren Zustand gebracht (kalte Redundanz). Bei den Bauteilen auf der SIL-Platine handelt es sich um sehr einfach und langlebige Bauteile mit einem eingeschränkten Funktionsumfang. In dieser Konfiguration erhält das System die SIL-Klassifizierung 2. Des Weiteren besteht die Möglichkeit, eine weitere Platine hinzuzufügen. Auf diese Weise ist es möglich, den Stellantrieb zu einem 1oo2-System zu machen und somit die SIL-Klassifizierung 3 zu erreichen.

Zwischenfazit

Die Recherche zu den zuvor genannten Beispielen ergab, dass das Vorgehen im Automobil-, sowie Luft- und Raumfahrtbereich die strengsten Sicherheitsanforderungen stellen. Dies hängt damit zusammen, dass Systemausfälle in diesen Bereichen mit hoher Wahrscheinlichkeit zu Personenschäden führen. Im industriellen Bereich hängt die Sicherheit primär vom Anwendungsfall ab. Aber auch hier sind Personenschäden grundsätzlich zu vermeiden. Der primäre Unterschied zu den anderen beiden Bereichen ist der zur Verfügung stehende Platz. Daraus folgt, dass häufig relevante System durch schiere „Masse“ abgesichert werden. Im industriellen Bereich ist es selten ein Problem, Teile einer Anlage doppelt auszulegen.
Da ein sicherheitsrelevanter PDU-C mit COTS-Komponenten im Raumfahrtbereich unüblich ist, ist es sinnvoll, das Konzept und die Schaltung so robust wie möglich auszulegen. Deshalb ist es sinnvoll eine Risikobewertung, wie im Automobil- oder Industriebereich üblich, anzufertigen. Des Weiteren ist es notwendig eine technisch einfache und sichere Fallbackfunktion bereitzustellen, da eine Grundfunktion auf jeden Fall gewährleistet werden muss. Diese Grundfunktionalität ist darüber hinaus eine Kernforderung der ECSS Standards. Es ist also das Ziel, die bewährte konventionelle Raumfahrttechnik mit neuen Ansätzen zu kombinieren, um so eine große Systemzuverlässigkeit bei gleichzeitig moderaten Kosten zu ermöglichen.

3 Systementwürfe

Wie bereits im Abschnitt 1.2 beschrieben, ist es zweckmäßig, verschiedene Systementwürfe zu realisieren. Beim Erstellen dieser Entwürfe ist sicher zu gehen, dass diese auch den Anforderungen entsprechen. Es ist notwendig, im Vorfeld die vorhandenen Risiken zu benennen, zu bewerten und zu dokumentieren. In Abschnitt 2.1 wurde eine Zusammenfassung über die verschiedenen Normen und ihre Planungswerkzeuge erarbeitet. Hierzu gehören die Machbarkeitsbewertung, FMEA, das Ursache-Wirkungs-Diagramm sowie der morphologische Kasten. Nachfolgend werden zum Erstellen und für die Bewertung der Konzepte diese Techniken zur Anwendung kommen. Zu Beginn jeder Methode wird darauf eingegangen, aus welchem Grund das gewählte Werkzeug zum Einsatz kommt und welche Ergebnisse zu erwarten sind.

3.1 Zugrunde liegendes PDU-Layout des Navigationssystems

In diesem Teil wird ein Überblick über den PDU-Entwurf von Kwiatkowski [17] gegeben. Die Abbildung 3.1 definiert die Schnittstellen der zu schaltenden PDU-Kanälen bzw. Datenleitungen für die Kommunikation. Dabei werden TTL(Transistor-Transistor Logik)-Signale zum Schalten der PDU-Kanäle verwendet. Für die Kommunikation mit den OBCs wurde ein RS422-Standard gewählt. Die Daten der PDU-Kanal-Überwachung (Monitor siehe Abbildung 3.1) sollen per UART (Universal Asynchronous Receiver Transmitter) gesendet werden.

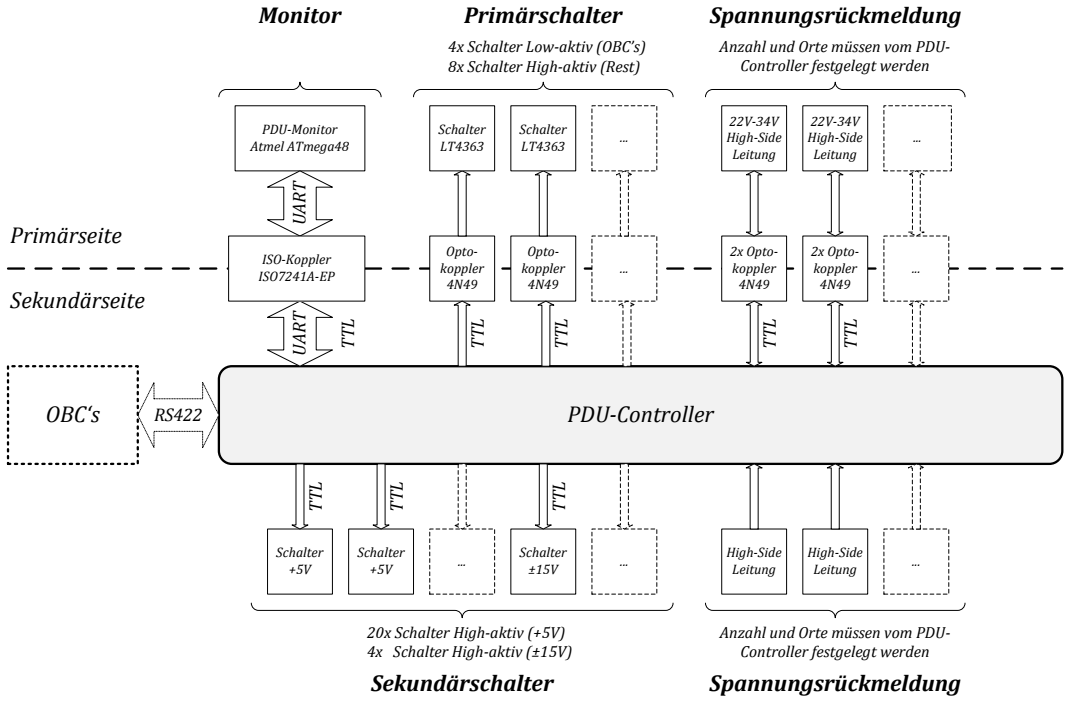


Abbildung 3.1: PDU-C Schnittstellen Übersicht

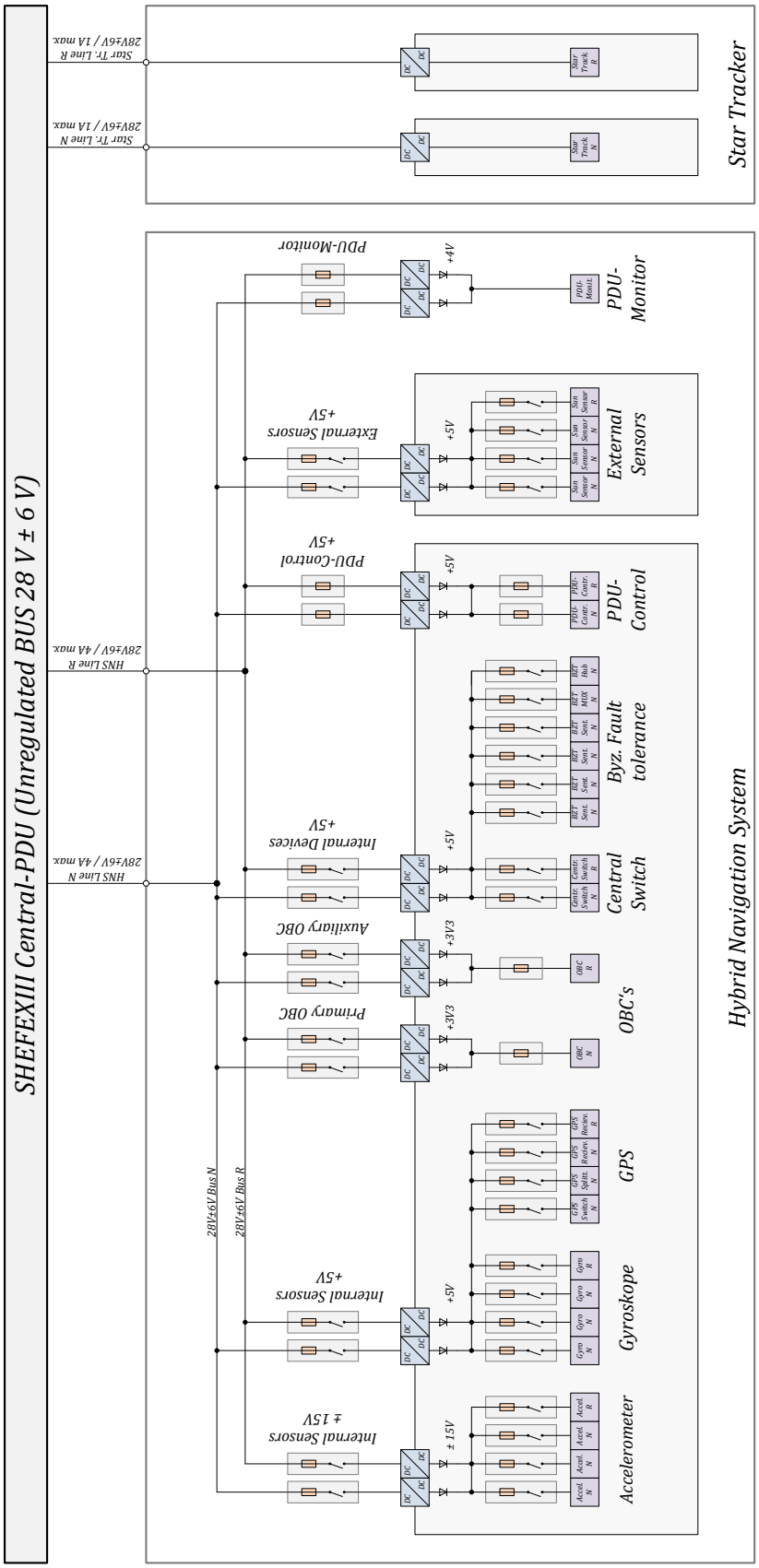


Abbildung 3.2: Systemarchitektur für die Leistungsversorgung des HNS (Hybrid Navigation System)[17].

Die Abbildung 3.2 zeigt den vereinfachten Aufbau der Energieversorgung der PDU, inklusive der Energieversorgung des PDU-C. Hieraus ist zu erkennen, dass die komplette Energieversorgung redundant, bis zu der Verteilung der einzelnen Komponenten ausgelegt worden ist. Eine weiterführende Redundanz ist nicht notwendig. Alle in dieser Abbildung dargestellten Sensoren sind so konzipiert worden, dass immer ein Sensor mehr, als für die Navigation notwendig vorhanden ist.
Sowohl die gesamten Sensoren, wie auch die in der Abbildung 3.2 dargestellte PDU sind nicht Bestandteil dieser Thesis sondern wurden durch die Bachelorthesis von Kwiatkowski [17] und dem Systemdesign vorgeben.

3.2 Risikolokalisierung mit einem Ursache-Wirkungs-Diagramm

Das Ursache-Wirkungs-Diagramm dient, ähnlich wie eine Mind-Map dazu, strukturiert Ideen zu sammeln, welche Ursachen zu einem bestimmten Ereignis führen können. Abhängig von der jeweiligen Quelle, ist das Ursache-Wirkungs-Diagramm, wie in dieser Ausarbeitung, Teil der FMEA oder geht dieser als eine von mehreren möglichen Methoden voraus. Ziel der Gruppe ist es, schnell mögliche Ausfallkriterien zu lokalisieren und diese Informationen anschließend für das weitere Vorgehen in der FMEA zu verwenden.

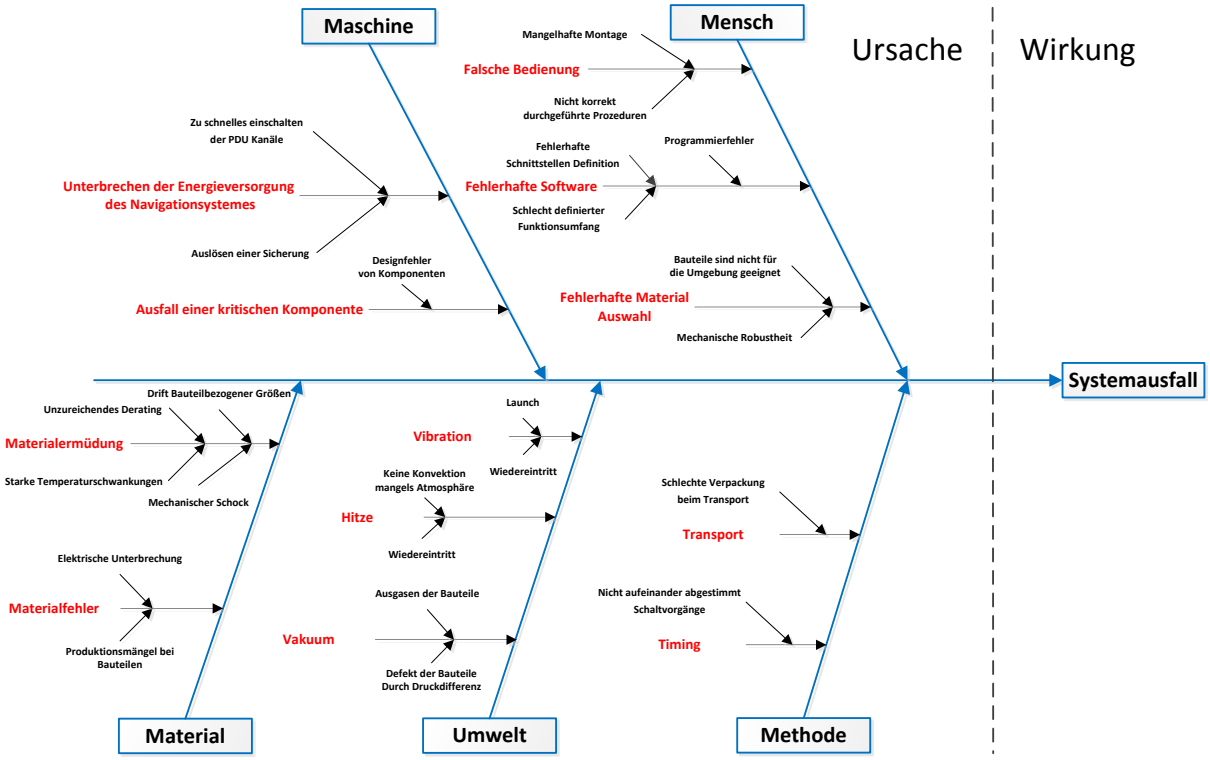


Abbildung 3.3: Darstellung möglicher Fehlerquellen in einem Ursache-Wirkungs-Diagramm

Die fünf im Ursache-Wirkungs-Diagramm verwendeten Oberkategorien werden im Buch von Tietjen, decker, Müller [30] empfohlen. Die so entstandene Struktur kann gleichzeitig als Gliederung für die FMEA verwendet werden.
Da es sich beim Ursache-Wirkungs-Diagramm um ein Werkzeug handelt, dass zur Ideenfindung verwendet wurde, ist davon auszugehen, dass nicht alle möglichen Fehlerquellen ermittelt worden sind. Dies ist aber zum Zeitpunkt der Konzeptplanung nicht notwendig, da noch nicht alle Missions- und Umgebungsparameter vollständig bekannt sind.

3.3 Fehlermöglichkeits- und -einflussanalyse

Bevor am Ende dieses Kapitels ein Konzept ausgewählt wird, wurde zunächst eine FMEA durchgeführt. Ziel der FMEA ist es, mögliche Risiken beim Betrieb für das System und für Personen vorzeitig zu erkennen und diese schon während der Planung zu berücksichtigen. Darüber hinaus soll durch die FMEA auch positiv Einfluss auf die Zuverlässigkeit genommen werden. Da es sich in dieser Bachelorthesis um die Entwickelung eines Konzeptes für ein sicherheitskritisches System handelt, ist das Verwenden einer Produkt-FMEA zweckmäßig. Hierbei ist zu beachten, dass der Begriff „Produkt-FMEA“ nicht geläufig ist. Verbreiteter ist der Begriff „System-FMEA“, welcher jedoch seit 2006 nicht mehr offiziell verwendet wird [34].
Zunächst wird das zuvor erstellte Ursache-Wirkungs-Diagramm als Grundlage verwendet, um die Spalten für *Fehlerort / Fehlermerkmal, potentielle Fehler* und *Fehlerursache* in der FMEA zu füllen. Da zu diesem Zeitpunkt noch keine Systementwürfe vorliegen, ist die Spalte *Potentielle Fehler* noch sehr allgemein gehalten. Anschließend sieht die FMEA vor, dass die Fehler gewichtet werden. Zu diesem Zweck liegt die folgende Bewertungsformel vor [34]:

$$\mathbf{RPZ} = A \cdot B \cdot E \tag{3.1}$$

Die Variable A (Tabelle 3.1) kennzeichnet die Wahrscheinlichkeit des Auftretens. Der Fehler B (Tabelle 3.2) sagt es etwas über die Schwere und die möglichen Folgen des Fehlers aus. Die Variable E (Tabelle 3.3) zeigt auf wie hoch die Wahrscheinlichkeit ist das der Fehler entdeckt wird und bewertet diesen. Der Wert RPZ (Risiko-Prioritätszahl Tabelle 3.2) gibt Auskunft über die Gefährlichkeit eines bestimmten Fehlers.

Die bei den Werten verwendeten Abstufungen, stammen in ihrer Grundform aus dem Buch VDA Band 4 Teil 2 [32]. Da sich die Beschreibungstexte des VDA auf die Automobilindustrie beziehen, mussten diese den vorherrschenden Gegebenheiten angepasst werden. Zu diesem Zweck wurde unter Zuhilfenahme der Bewertungszahlen der Firma Riedel GmbH [11] und eigener Formulierungen Änderungen vorgenommen. Alle vier nachfolgenden Tabellen sind auf diese Weise entstanden. Die ECSS Norm ECSS30-02C [29] sieht für die Durchführung und die Bewertung der FMEA ein abweichendes Verfahren vor. Die FMEA wurde nach den Verfahren der Automobil- und Prozessindustrie durchgeführt. Ferner ist die Einteilung der FMEA, wie sie in diesem Fall vorgenommen wurde, feiner und erhöht somit die Anwendbarkeit(2.1).

Tabelle 3.1: Skalierungstabelle für die Auftrittswahrscheinlichkeit der folgenden FMEA

Wahrscheinlichkeit des Auftretens (A)		
Einfache-	**Allgemeine-Bewertungskriterien**	**Punkte**
sehr gering	Es ist unwahrscheinlich, dass der Fehler auftritt.	1
gering	Der Fehler wird nur in ganz geringem Umfang auftreten.	2-3
mäßig	Der Fehler wird hin und wieder auftreten.	4-6
hoch	Der Fehler tritt häufig auf.	7-8
sehr hoch	Es ist nahezu sicher, dass der Fehler auftreten wird.	9-10

Tabelle 3.2: Einteilung der Bedeutungsstufen für die folgende FMEA

Bedeutung (B)		
Einfache-	**Allgemeine-Bewertungskriterien**	**Punkte**
sehr gering	Es ist unwahrscheinlich, dass der Fehler irgendeine wahrnehmbare Auswirkung haben wird.	1
gering	Der Fehler ist unbedeutend, das System wird nur geringfügig tangiert.	2-3
störend	Der Fehler ist mittelschwer, Funktionsfähigkeit ist gegeben, Einschränkungen von wichtigen Bedien- und Sensorsystemen.	4-6
hoch / kritisch	Gefahr von Verletzungen und Dauerschäden, Umweltbelastung, Funktionsfähigkeit des Systems oder von Teilsystemen eingeschränkt, starke Beeinträchtigung der Arbeitsbedingungen.	7-8
sehr hoch / katastrophal	Lebensgefahr, Gefahr schwerer Umweltschäden, Gefahr schwerer Verletzungen und Dauerschäden, Gefahr für Umwelt mit Folgeschäden.	9-10

Tabelle 3.3: Aufteilung für die Entdeckungswahrscheinlichkeit der folgenden FMEA

Wahrscheinlichkeit der Entdeckung (E)		
Einfache-	**Allgemeine-Bewertungskriterien**	**Punkte**
sehr hoch	Es ist sicher, dass der Fehler entdeckt wird, da der nachfolgende Arbeitsgang nicht fortgeführt werden kann, wenn der Fehler vorhanden ist.	1
hoch	Der Fehler ist so offensichtlich, dass er am nachfolgenden Arbeitsgang auch ohne geplante Prüfung entdeckt wird.	2-3
mäßig	Der Fehler ist bei aufmerksamer Betrachtung bei nachfolgenden Arbeitsgängen zu erkennen und wird spätestens bei der Endprüfung im Warenausgang entdeckt.	4-6
gering	Der Fehler könnte nur bei 100 % Prüfung sicher entdeckt werden.	7-8
sehr gering	Entdecken der aufgetretenen Fehlerursache ist unwahrscheinlich, die Fehlerursache wird oder kann nicht geprüft werden.	9-10

Tabelle 3.4: Farbliche und Nominal Einteilung der RPZ

RPZ Risiko-Prioritätszahl (RPZ)		
Häufigkeit	**Wert**	**Farbe**
hoch	<= 1000	
mittel	<= 250	
gering	<= 125	
klein	<= 1	

Obwohl bei der Erstellung der Tabelle 3.4, die Quelle [32] verwendet wurde, ist die Unterteilung nicht eindeutig. In der Literatur [34, 30, 32] sind unterschiedliche Einteilungen vorhanden. Diese Unterschiede sind in der Praxis jedoch nicht weiter von Bedeutung. Eine Erläuterung zu diesem Umstand folgt im Zwischenfazit dieses Abschnitts.

HSB Hochschule Bremen City University of Applied Sciences — DLR

Produkt FMEA: SHEFEX III

Name / Abteilung: GNC | **Erstellt durch: Lars Johannsen** | **Datum: 07.06.2015**

	Fehlerort / Fehlermerkmal	Potentielle Fehler	Fehlerfolge	Fehlerursache	A	B	E	RPZ	Empfohlene Maßnahmen	Verantwortlich
1	Maschine	Unterbrechen der Energieversorgung des Navigationssystems	Ausfall der PDU / PDU-C	Zu schnelles einschalten der PDU Kanäle	3	4	1	12	Das Gesamte Navigationssystem ausgibig testen um die Leistungsaufnahme zu ermitteln	Projektleitung
2			Ausfall des PDU-C	Auslösen einer Sicherung	3	7	4	84	Die Grundfunktionalität beim Ausfall des PDU-C muss weiterhin gegeben sein.	PDU-C Konzept
3		Ausfall einer kritischen Komponente	Ausfall von Sensoren durch eine defekte Ansteuerung	Designfehler von Komponenten	4	2	8	64	Da die Sensoren ein Fehlertollerant sind ist der Ausfall folgenlos. Teilweise wird dieser sogar erwartet.	GNC
4	Mensch	Falsche Bedienung	Verbindungen lösen sich / die Funktion ist nicht gegeben	Mangelhafte Montage	4	7	10	280	Für die Montag müssen gute Prozeduren erstellt und eingehalten werden	Projektleitung / Konstruktion
5			Es wird zuviel Energie beim Betrieb benötigt.	Nicht korrekt durchgeführte Prozeduren	3	7	6	126	Genaue Qualitätskontrollen durch die Fachabteilungen / exakte Schnittstellendefinition	Projektleitung / Fachabteilungen / PDU-C Konzept
6		Fehlerhafte Software	Fehlfunktion des PDU-C	Fehlerhafte Schnittstellen Definition	4	4	6	96	Genaue Funktionsbeschreibung der Sensoren und Schnittstellen	Systemingenieur
7			Fehlfunktion des PDU-C oder Ausfall	Programmierfehler	9	8	1	72	Verwenden des V-Model und der DO-178, sowie umfandes Tests	Programmierer / Systemingenieur
8			zu hoher Energie verbrauch / System hat Fehlfunktion	Schlecht definierter Funktionsumfang	5	4	7	140	Genaue Funktionsbeschreibung der Sensoren und Schnittstellen	Systemingenieur
9		Fehlerhafte Material Auswahl	Systemteile fallen beim Betrieb aus.	Bauteile sind nicht für die Umgebung geeignet	6	7	10	420	Für anfällige Komponenten ist immer eine Redundanz oder Degratation vorsehen	PDU-C Entwurf
10			Kurzschluss / Systemausfall	Mechanische Robustheit	3	8	9	216	Rechtzeitige zusammen Arbeit zwischen Entwicklern der PDU-C Hardware und Konstruktion	PDU-C Hardware / Konstruktion
11	Material	Materialermüdung	Durchbrennen von Bauteilen / Spannungspitzen	Unzureichendes Derating	4	7	3	84	Zum Bestimmen von Bauteiltolleranzen bzw. deren Auslegung gibt es Tabellen mit Empfehlungen	PDU-C Hardware / PDU Hardware
12			Timing-Probleme / Ausfall von Komponenten	Drift bauteilbezogener Größen	3	6	6	108	Verwendung von qualifizierten Bauteilen / Notbetrieb muss gewährleistet werden.	PDU-C Hardware / PDU-C Konzept / PDU Hardware
13			Überhitzung von Bauteilen	Starke Temperatur-schwankungen	5	8	9	360	Auf den Wirkungsgrad von Bauteilen achten / Konzept zum Wärmemanagement muss erstellt werden. Grundfunktionalität muss erhalten bleiben.	PDU-C Hardware / PDU Hardware / Konstruktion / PDU-C Konzept
14			Defekt von Systemen und mechanischen Strukturen	Mechanischer Schock	4	8	10	320	Bauteile müssen mechanische Belastungen ertragen / Notbetrieb muss gewährleistet werden.	PDU-C Hardware / PDU Hardware / Konstruktion / PDU-C Konzept
15		Materialfehler	Signalverlust / Kurzschluss	Elektrische Unterbrechung	4	3	10	120	QM für elektrische Verbindungen muss durchgeführt werden / Notbetrieb muss gewährleistet werden.	PDU-C Hardware / PDU-C Konzept
16			Systemausfall / Teilsystemausfall	Produktionsmängel bei Bauteilen	3	3	10	90	Qualifizierte Bauteile verwenden / Notbetrieb muss gewährleistet werden.	PDU-C Hardware / PDU-C Konzept
17	Umwelt	Vakuum	Systemausfall / Teilsystemausfall	Defekt der Bauteile Durch Druckdifferenz	5	8	2	80	Bei der Auswahl der Bauteile auf ihre Bauart achten ggf. Thermal Vakuum Test durchführen	PDU-C Hardware / PDU Hardware / GNC
18			Beeinträchtigung der Sensoren	Ausgasen der Bauteile	1	3	10	30	Bei der Auswahl der Bauteile auf ihre Bauart achten ggf. Thermal Vakuum Test durchführen	PDU-C Hardware / PDU Hardware / GNC
19		Hitze	Bauteilausfall durch Überhitzung	Keine Konvektion mangels Atmosphäre	5	4	10	200	Auf den Wirkungsgrad von Bauteilen achten / Konzept zum Wärme Management muss erstellt werden. Grundfunktionalität muss erhalten bleiben.	PDU-C Hardware / PDU Hardware / PDU-C Konzept / GNC
20			Bauteilausfall durch Überhitzung / ggf. Verglühen von Sensoren	Wiedereintritt	9	3	10	270	Auf den Wirkungsgrad von Bauteilen achten / Konzept zum Wärme Management muss erstellt werden. Grundfunktionalität muss erhalten bleiben.	PDU-C Hardware / PDU Hardware / PDU-C Konzept
21		Vibration	Sensordrift / Teil Systemausfall	Wiedereintritt	9	8	1	72	Kontrolle der Messdaten auf Logik / Verwendung von Vibration unempfindlich Bauteilen	PDU-C Hardware / PDU Hardware / PDU-C Konzept
22			Sensordrift / Teil Systemausfall	Launch	9	8	1	72	Kontrolle der Messdaten auf Logik / Verwendung von Vibration unempfindlich Bauteilen	PDU-C Hardware / PDU Hardware / PDU-C Konzept
23	Methode	Timing	PDU-Kanäle haben einen undefinierten Zustand / Energieverbrauch ggf. zu hoch	Nicht aufeinander abgestimmt Schaltvorgänge	10	8	3	240	Durch das Schaltungsdesign werden undefinierte Zuständen unterbunden. Ausgiebige Tests sind notwendig	PDU-C Hardware / PDU Hardware / PDU-C Konzept
24		Transport	Transportschäden am Navigationsystem	Schlechte Verpackung beim Transport	4	7	8	224	QM befragen, von Erfahrungen aus früheren Projekten profitieren / Prozeduren erstellen	Projektleitung / Systemingenieur

Abbildung 3.4: Zusammenstellung aus den Daten des Ursache-Wirkungs-Diagramm (3.3)

Erläuterung der potenziellen Fehler

Aufgrund der gewählten Darstellungsweise in Abbildung 3.4 [9] sind die Beschreibungen für Fehler und deren Ursache sehr kurz zusammengefasst. Daher werden alle rot umrandeten potenziellen Fehler noch einmal genauer erklärt. Bei den rot umrandeten Fehlern ist es möglich, durch ein PDU-C Konzept Einfluss auf die Häufigkeit der Fehler zu nehmen. Die nicht markierten

Ursachen, fallen in die Zuständigkeit anderer Projektbereiche. Dies ist keine Wertung der Relevanz der Probleme. Infolgedessen werden diese mögliche Fehlerquellen an die entsprechenden Personen zwecks Verbesserung der Zuverlässigkeit weitergeleitet.

- **2. Auslösen einer Sicherung -** Eine Sicherung in der Zuleitung des PDU-C oder des Navigationssystems löst aus (siehe Abschnitt 3.1). Dies kann sowohl durch eine Überlastung des PDU-C passieren, aber auch Kurz-, Körper-, Leitungs- und Erdschluss sind möglich.
- **5. Nicht korrekt durchgeführte Prozeduren -** Eine der Hauptaufgaben des PDU-C ist es, während des Systemstarts den Strombedarf, durch ein sequenzielles Einschalten der einzelnen Verbraucher, die Stromaufnahme nicht über 4 A steigen zu lassen.
- **9. Bauteile sind nicht für die Umgebung geeignet -** Durch das teilweise Verwenden von COTS-Komponenten ist davon auszugehen, dass die auszuwählenden Komponenten nicht allen Anforderungen der Raumfahrt genügen werden. Ferner ist es auch nicht möglich, diese Teile zu verifizieren, da dieser Vorgang kosten- und zeitintensiv ist. Somit muss ein Ausfall einer solchen Komponente eingeplant werden.
- **12. Drift[8] bauteilbezogener Größen -** In dem zu entwickelnden Navigationssystem, kommen Bauteile zum Einsatz (z. B. der Oszilatorquarz), die Faktoren wie Vibration oder Alterung unterliegen. Es muss folglich der Drift, der auf die Komponenten wirkt, mit berücksichtigt werden. Sonst ist es möglich, dass es so zu Timing Problemen und/oder Signalverlust kommen kann.
- **13. Starke Temperaturschwankungen -** Die durch die verschiedenen Stufen einer Mission, wie SHEFEX III, hervorgerufenen Temperaturschwankungen, können zu einer Überhitzung der Bauteile führen. Es ist wichtig, bei der Auswahl der Bauteile auf einen zweckmäßigen Wirkungsgrad zu achten, damit nicht unnötig Energie in Wärme umgewandelt wird. Des Weiteren ist zu erwarten, dass sich die Materialien durch die Temperaturschwankungen ausdehnen bzw. zusammenziehen werden. Diese Parameter müssen bei der Entwicklung beachtet werden bzw. vor dem Start in einer Thermal-Vakuumkammer getestet werden.
- **14. Mechanischer Schock -** Der Start der Rakete, die Landung sowie das Abtrennen der Raketenstufen können Komponenten beschädigen oder falsche Telemetriedaten verursachen.
- **15. Elektrische Unterbrechung -** Es ist denkbar, dass es auf Grund schlechter Verarbeitung bei der Montage, als auch bei den Bauteilen selbst, zu Signalverlusten kommen kann. Die Gründe hierfür sind vielfältig, wie z. B. ein Wackelkontakt oder eine gebrochene Leiterbahn. Ein solches Ereignis sollte nur geringe Auswirkungen auf das System haben.
- **16. Produktionsmängel bei Bauteilen -** Bei jedem Bauteil kann es Schwankungen in der Qualität geben. Daher kann es zu Ausfällen von Bauteilen kommen. Dies darf nicht zu einem Ausfall des gesamten Navigationssystems führen.

8 Der Begriff „Drift“ bezeichnet in diesem Zusammenhang die Abweichung einer wichtigen Kenngröße eines Bauteile aufgrund von Alterung oder äußeren Einwirkungen.

- **19. Keine Konvektion mangels Medium (Atmosphäre) -** Da es im luftleeren Raum keine Konvektion mit einem Umgebungsmedium gibt, erfolgt in diesem Fall die Wärmeableitung primär nur über Infrarotstrahlung. Die Folge hieraus ist, dass es ein Konzept zur Ableitung von thermischer Wärme geben muss.
- **20. Wiedereintritt (Hitze) -** Die beim Wiedereintritt entstehenden Temperaturen können, abgesehen von der steigenden Temperatur im Inneren von SHEFEX III, auch direkte Schäden an der Außenseite verursachen. Es wird zum Beispiel damit gerechnet, dass die Star-Tracker[9] zerstört werden. Dieser Defekt darf allerdings nicht zu einem Kurzschluss des Navigationssystems führen. Weiterhin dürfen falsche Messwerte nicht in die Navigation mit einfließen.
- **21.-22. Launch/Wiedereintritt (Vibration) -** In dem zu entwickelnden Navigationssystem, werden Bauteile zum Einsatz gebracht, die Faktoren wie Vibration und Hitze unterliegen. Folglich muss der Drift, der bei den Komponenten entsteht, mit berücksichtigt werden. Diese Fehlerquelle ist nicht zu unterschätzen, da sowohl beim Start als auch beim Wiedereintritt Vibrationen mit hohen Frequenzen entstehen können.
- **23. Nicht aufeinander abgestimmte Schaltvorgänge -** Um bei dem Systemstart, sowie dem Betrieb des Navigationssystems die maximale Stromaufnahme nicht zu überschreiten, ist es notwendig, eine Startup-prozedur zu entwickeln und diese zu testen, um mögliche Fehlerquellen zu identifizieren.

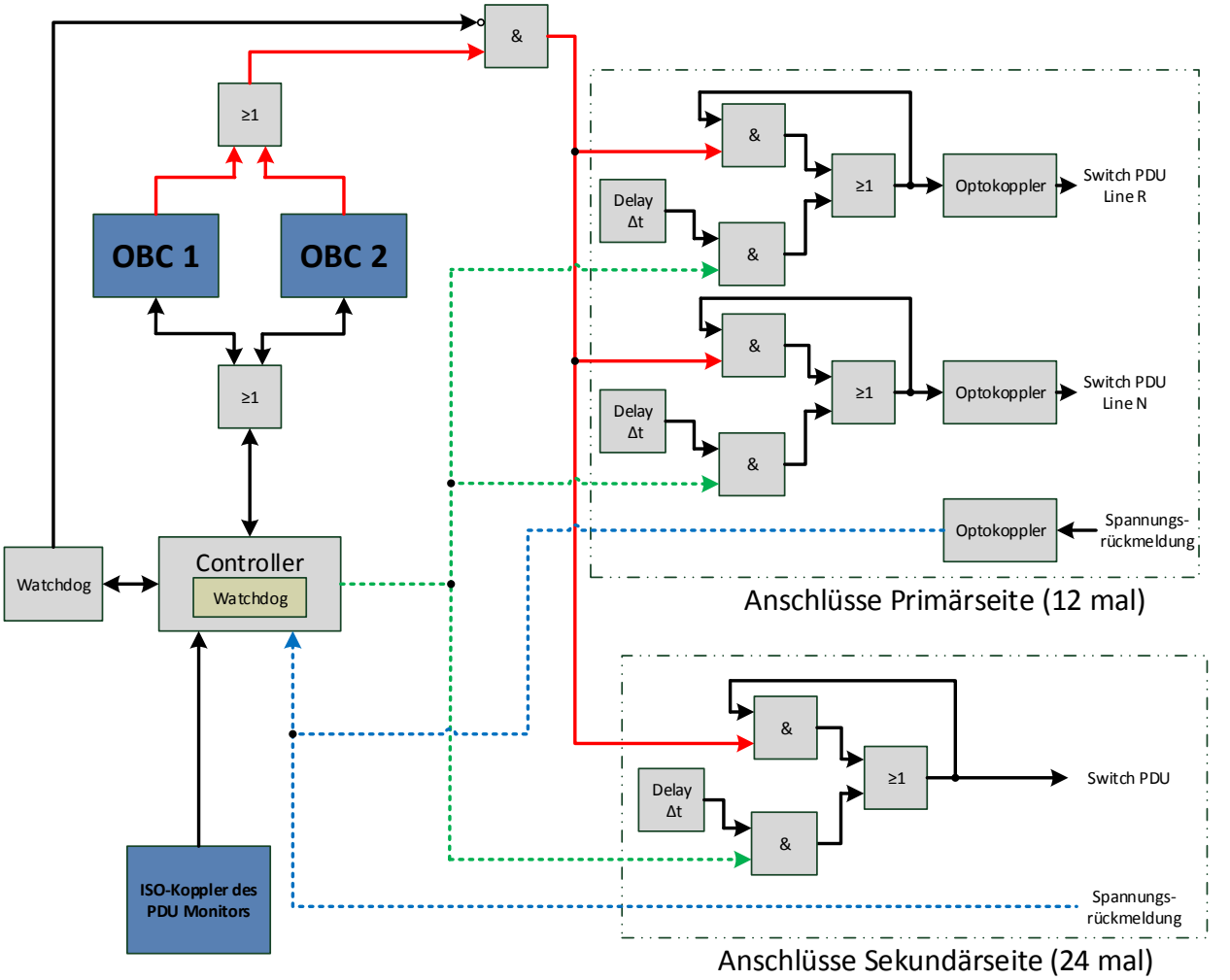
Zwischenfazit

An dieser Stelle ist die FMEA noch nicht beendet, da die noch folgenden Konzepte abermals in dieser FMEA untersucht werden müssen. Dieser Vorgang soll nachweisen, dass die erstellten Konzepte eine Verbesserung in der Zuverlässigkeit und Sicherheit erbracht haben. Für eine bessere Verständlichkeit der Daten ist es zielführend, die bisher erlangten Ergebnisse zu erläutern. Da es noch keine festen Missions-Parameter gibt, ist der erzielte RPZ-Wert in seiner Aussagekraft fragwürdig. Des Weiteren ist der RPZ-Wert immer vom subjektiven Empfinden seiner Ersteller abhängig. Aus diesem Grund gibt es die Möglichkeit eine FMEA so durchzuführen, dass die Gewichtung der einzelnen Komponenten (A-, B- und E-Wert) der RPZ bei der Rangfolge mit berücksichtigt werden. Ferner ist es in manchen Industriebereichen üblich, A-, B- und E-Werte durch eine vorangegangene Formel zu ermitteln. Hierzu werden Parameter, wie beispielsweise die Verfügbarkeit eines Produktes mit berücksichtigt. Da für den PDU-C Entwurf zu diesen Zeitpunkt derartige Parameter noch nicht bekannt sind, wurde auf die Verwendung verzichtet. Auch die Literatur [19, 34, 30] weist darauf hin, dass die durch eine FMEA ermittelten Ergebnisse in ihrer Skalierung immer kritisch betrachtet werden sollen und dabei „der gesunde Menschenverstand“ eingesetzt werden muss. Trotzdem sind die Ergebnisse der FMEA eine gute Arbeitsgrundlage. Durch den Ideenaustausch mit anderen Kollegen konnten auf diese Weise Fehler entdeckt werden, die zuvor nicht bedacht wurden.

9 Bei einem Star Tracker handelt es sich um eine Kamera die Bilder von Sternen macht. Anhand dieser Bilder kann die Lage im Raum bestimmt werden.

3.4 Konzept 1: Minimalentwurf

Beim ersten Konzept handelt es sich um einen Minimalansatz. Der Gedanke, der diesem Design zugrunde liegt, ist der Versuch ein System so einfach wie möglich zu gestalten und trotzdem den Anforderungen gerecht zu werden. Die hierbei verwendete minimale Anzahl von Komponenten führt zu einer erhöhten Ausfallsicherheit des Systems.



SHEFEX III

Legende:

Systemvorschlag 1 PDU-Controller

- Externe Komponenten die nicht Teil des PDU-C-Systems sind.
- Schaltbefehle, Messdaten, TTL-Logik
- Notfunktions-I/O Leitung wird freigegeben bei PDU-C-Ausfall
- Parallele Controller I/O Verbindung (jeder Schalter ist einzeln anzusteuern und wird nur zur Übersicht als eine Verbindung dargestellt.)
- Rückmeldung I/O Signal (jeder Schalter liefert separat ein Signal und wird nur zur Übersicht als eine Verbindung dargestellt.)

DLR Deutsches Zentrum für Luft- und Raumfahrt

HSB Hochschule Bremen City University of Applied Sciences

Abbildung 3.5: Minimalkonzept zur Entwicklung einer PDU-C Schaltung

Der in Abbildung 3.5 dargestellte Systemvorschlag stellt den PDU-C dar. Zu der PDU sind die Systemgrenzen in Abbildung 3.1 dargestellt. Sie werden im Entwurf durch die Optokoppler und den Iso-Koppler dargestellt. Auf der Sekundärseite werden die Signalleitungen durch Verbinder dargestellt. Die Unterscheidung zwischen Primär- und Sekundärseite wird in Darstellung 3.2 erläutert. Die Abbildung ist Bestandteil der Bachelorthesis von Kwiatkowski [17]. Des Weiteren ist in dieser Thesis ein Erdungskonzept des gesamten Navigationssystems enthalten. Mittels mehrerer DC/DC-Wandler wird das Navigationssystem galvanisch vom Rest des SHEFEX III-Systems getrennt. Um diese Trennung aufrecht zu erhalten, ist es notwendig, alle Signale zur Primärseite und zum PDU-C ebenfalls galvanisch zu trennen. Die Primärseite beinhaltet, wie in Illustration 3.2 dargestellt, jede Komponente, die den DC/DC-Wandler voran geschaltet ist. Die Sekundärseite ist zusätzlich durch einen Kasten gekennzeichnet, auf dessen Grenze die DC/DC-Wandler dargestellt sind.
Die OBCs sind ebenfalls als gegeben anzusehen und nicht Bestandteil des PDU-C Konzeptes.

Beim Start des Navigationssystems wird zunächst die Energie durch die zentrale Energieversorgung von SHEFEX III bereit gestellt. Dabei werden die OBCs automatisch, ohne Schaltvorgang des PDU-C, eingeschaltet. Der PDU-C wird hierbei ebenfalls gestartet. Da die Schalter jedoch zum Teil low-aktiv sind, ist es notwendig einen undefinierten Zustand bzw. einen Schaltvorgang zum Zeitpunkt des Systemstarts zu verhindern. Ein undefinierter Zustand hätte zur Folge, dass es bei den low-aktiv Schaltern zu einem ungewollten Systemstart einzelner PDU Kanäle kommen kann. Um dies zu verhindern, muss ein Zeitbaustein vorgesehen werden, der den Schaltern ein high-signal für eine kurze Zeit vorgibt bis der PDU-C betriebsbereit ist. Diese Zeitbausteine wurden im PDU-C Entwurf durch ein Δt gekennzeichnet. In der Bachelorthesis von Kwiatkowski[17] sind, zusätzlich zu den low-aktiv Schaltern, high-aktiv Schalter vorgesehen. Diese sind im PDU-C-Entwurf nicht näher gekennzeichnet, um die Übersichtlichkeit des Konzeptes zu erhöhen. Auch bei diesen ist es denkbar, ein Schaltsignal beim Systemstart zu unterdrücken um auch hier einen definierten Zustand herzustellen. Der technische Aufwand für diesen Vorgang kann, je nach Schaltungsdesign, klein gehalten werden, da der Zeitgeber an einer zentralen Stelle im System angebracht werden kann. Von dort kann das Signal weiter an die einzelnen Schalter verteilt werden. Es ist nicht notwendig, diesen Zeitgeber ausfallsicher oder redundant zu gestalten. Diese Aufgabe nur einmal beim Systemstart durchgeführt und danach nicht mehr benötigt. Sollte der Zeitgeber dennoch vor dem Start einen Defekt aufweisen, zieht dies zwar ggf. einen Abbruch des Starts nach sich, jedoch nicht einen Verlust der Mission.
Ein weiterer Teil des PDU-C Schaltungskonzeptes ist der Controller. Der Controller ist der wichtigste Teil des Konzeptes. Seine Funktionsfähigkeit muss unter allen Umständen gewährleistet werden. Da dies auf Grund der Tatsache, dass es keine Redundanz oder Fehlertoleranz gibt, nicht möglich ist, wird das Prinzip der Degradation angewandt. Auf der Darstellung sind zwei Watchdogs[10] zu erkennen. Der integrierte Watchdog überwacht, ob der auszuführende Code auf dem PDU-C abgestürzt ist und erzeugt daraufhin einen Interrupt. Der Funktionsumfang des externen Watchdogs kann stark variieren. Die Funktion kann von einer einfachen Spannungsüberwachung, bis hin zu einer Kontrolleinheit reichen, die die Rechnungen des Controllers kontrolliert. Des Weiteren hängt der Funktionsumfang von der Auswahl des Controllers ab, was

10 Ein Watchdog oder auch WDC ist eine Schaltung oder ein Softwarecode der eine überwachende Funktion einnimmt. Tritt ein Fehler auf, signalisiert der Watchdog dies einem übergeordnetem System. Der Funktionsumfang kann dabei je nach Bauteiltyp stark variieren.

im Abschnitt 3.8.1 genauer betrachtet wird. Ergänzend zu der im ersten Konzept gezeigten Konstellation aus Mikrocontroller und Watchdog, wäre es unter Umständen zielführender, anstelle einem Watchdog, drei zu verwenden. Diese würden in einer 2oo3 (Abschnitt 2.2.4) Verschaltung zusammenarbeiten. Dies würde die Ausfallwahrscheinlichkeit weiter senken. Hierbei ist jedoch zu beachten, dass je nach Typ der verwendeten Watchdogs und deren Aufgaben, die benötigte Voterlogik sehr komplex werden kann. Aus diesem Grund, wurde bei diesem Konzept darauf verzichtet.
Erkennen die Watchdogs einen Fehler des PDU-C, geben sie die Notfunktion des PDU-C Systems frei. Die OBCs besitzen jeweils ein Ausgangssignal, dass nach dem Start aktiviert wird. Diese Leitung dient dazu, im Falle eines Fehlers des PDU-C, die Kontrolle über die PDU Schalter zu übernehmen. Gemeinsam mit dem Watchdog-Signal schaltet das OBC-Signal alle Schalter ein. Dieses Verfahren erlaubt, dass die Funktionsfähigkeit des Navigationssystems weiter erhalten bleibt. Durch jenen Vorgang ist es nicht mehr möglich, einzelne Schaltvorgänge vorzunehmen. Das Navigationssystem wäre weiterhin funktionsfähig. Der PDU-C hat sich somit selbst degradiert und erfüllt damit die Forderung nach einem intrinsischen Degradationskonzept. Ferner ist das PDU-C Konzept in Kombination mit den OBCs ein-Fehlertolerant. Das PDU-C System für sich selbst betrachtet ist nicht Ein-Fehlertolerant. Es ist aber in diesem Fall zweckmäßig beide Navigationssystemteile gemeinsam zu betrachten, da ein Ausfall beider OBCs sehr unwahrscheinlich ist und in jedem Fall zu einem Missionsfehlschlag führen würde.
Der Einsatz dieser Notfunktion ist jedoch nur möglich, nachdem das System zuvor alle Schalter einmal aktiviert hat. Diese Schutzmaßnahme wird damit begründet, dass das Aktivieren dieser Funktion beim Systemstart dazu führt, dass die Energieaufnahme zu hoch wäre. Dies führt zu einem Abschalten des gesamten Navigationssystems, was zu vermeiden ist. Des Weiteren beinhaltet das PDU-C eine Spannungsrückmeldung von den PDU-Schaltern und dem PDU-Monitor. Der PDU-Monitor hat die Aufgabe Messdaten über Strom und Spannung aus der PDU zu sammeln sowie so dem PDU-C zu ermöglichen ggf. Schaltsignale selbstständig zu koordinieren oder die Messdaten aufzuzeichnen. Die Spannungsrückmeldung ist vorgesehen, um zu überprüfen, ob der Schaltbefehl der PDU-C funktioniert hat und somit auch, ob die PDU den Kanal geschaltet hat.
An dieser Stelle wird folgend dem Auswahlprozess eines Konzeptes (Abschnitt3.10) etwas vorweggenommen. Dies ist notwendig, um einen wichtigen Hinweis zu geben. Dieses Konzept kommt nur in Frage, da nur in Verbindung mit den OBCs die Anforderung der ein-Fehlertoleranz erfüllt wird.

Erläuterung zu Designgrundlagen

Die Erstellung des ersten Konzeptes warf bereits eine grundsätzliche Designentscheidung auf, die maßgeblich von der Auswahl eines Controllers abhängt. Sofern die Wahl auf eine Einheit mit vielen Ausgängen fällt, hat der Entwickler die Möglichkeit, jeden Schalter einzeln anzusteuern. Dieses hat jedoch den Nachteil, dass aufgrund der vielen Signalleitungen, die später zu erstellende Schaltung zu groß ist. Entscheidet man sich dagegen für eine kleinere Einheit mit weniger Ausgängen ist diese vielleicht robuster, weil die Technik älter und bewährter ist. Gleichzeitig kann es allerdings vorkommen, dass nicht mehr jeder Kanal einzeln angesteuert werden kann. Technisch gesehen stellt das kein Problem dar. Es besteht weiterhin die Möglichkeit über einen Datenbus die Schaltsignale zu verteilen und nachfolgend über ein Register oder die Schalter über einen Slave-Controller zu betätigen. Daraus folgt jedoch, dass ein weiteres Bauteil in Reihe geschaltet wird, der digitale Steuersignale (Bus-Signal) für die PDU-Schalter wieder in analoge umwandelt, um so die Optokoppler ansteuern zu können. Dieses Bauteil führt dazu, dass die Zuverlässigkeit geringer wird im Vergleich zu einem einzelnen Bauteil.
Wie in dem Buch von Flühr [8] beschrieben, ist es nicht möglich, bei komplexen Systemen eine Sicherheit zu 100 % zu garantieren. Folglich lässt sich auch nicht bestimmen, wie ausfallsicher ein komplexes Bauteil ist. Betrachtet man nun die Beispiele von sicherheitsrelevanten Systemen (Abschnitt 2.4, Flühr [8]), dann ist festzustellen, dass diese häufig sehr einfach sind und auf eine hohe technische Komplexität bewusst verzichtet wird. Der erste Entwurf soll aus diesem Grund so aufgebaut werden, dass die Aufgabe mit einem minimalen Aufwand erfüllt werden kann.

3.5 Konzept 2: Maximale Ausfallsicherheit

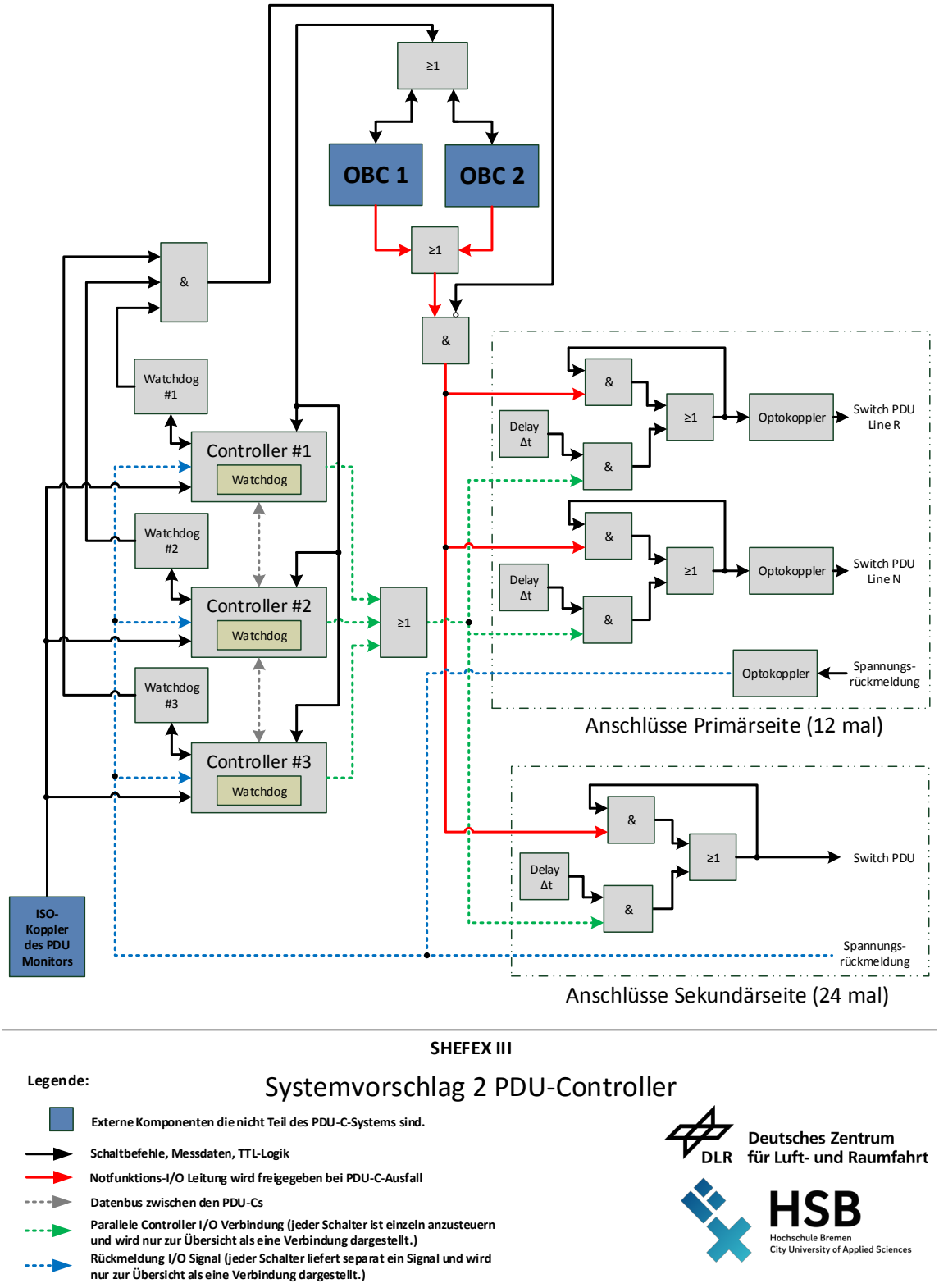


Abbildung 3.6: Konzept 2: maximale Ausfallsicherheit

Das zweite Konzept ähnelt in einigen Teilen dem ersten Konzept (Illustration 3.5). Folglich werden die bereits erwähnten Teile in diesem Teil nicht mehr behandelt, da ihre Funktion identisch der im ersten Konzept ist. Dazu gehören:

- OBCs
- PDU-Monitor
- Primär-Schalter
- Sekundär-Schalter
- OBC-Notschaltung beim Ausfall des PDU-C

Das zweite Konzept verwendet eine Kombination aus drei Controllern. Diese Form ist häufig zu finden, wenn das Thema Redundanz von Bedeutung ist. Als Vorlage diente dabei der Konferenzbeitrag *A fault-tolerant embedded microcontroller testbed* [26].
Zu Beginn der Erläuterung wird auf die drei externen Watchdogs eingegangen. Da es abweichend zum ersten Systemvorschlag, drei Controller gibt, sind auch drei Watchdogs vorgesehen. Ihre Aufgabe bleibt weiterhin sehr abhängig von der Auswahl des Watchdogtypen. Dennoch sollte eine Funktion immer enthalten sein: Der Controller muss ein Heartbeat-Signal an die Watchdogs senden. Durch ein Heartbeat Signal (Pulssignal) wird dem Watchdog signalisiert, dass der Controller nicht stehen geblieben ist und weiterhin Berechnungen durchführt. Ist dies nicht der Fall, ist der Watchdog in der Lage den Controller zu zurückzusetzen. Weiterhin wird das Reset-Signal auch verwendet, um die Notfunktion der OBCs freizugeben. Abweichend vom ersten Konzept ist hier jedoch nicht das Reset-Signal eines Watchdogs notwendig, sondern das aller drei Watchdogs. Dies hat zur Folge, dass erst alle drei Controller ausgefallen sein müssen, bevor die Notfunktion freigegeben wird. Das Konzept von Watchdogs hat jedoch den Nachteil, dass es nicht möglich ist, dass ein Watchdog logische Fehler erkennt. In der einfachsten Ausführung ist auch das Erkennen von Latch-up[11] oder das Kippen eines Bits nicht detektierbar.
Alle drei Controller sind durch Datenleitungen miteinander verbunden und überwachen sich gegenseitig. Die Controller führen identische Operationen aus und vergleichen diese nachfolgend miteinander. Das Ausgangssignal wird erst dann gesendet wenn alle Controller zum gleichen Ergebnis kommen. Durch dieses Verfahren entfällt auch die Notwendigkeit eines Voters, was den Wegfall eines Single Point of Failure bedeutet. Jedoch entsteht durch dieses Verfahren eine neues Problem. In einer solchen Konstellation von drei Controllern ist es notwendig, dass es immer einen Mastercontroller gibt. Wird dieser Mastercontroller statisch festgelegt, hat dessen Ausfall den Ausfall des Systems zur Folge. Es ist also notwendig, die Funktion das Masters unter den Controllern rotieren zu lassen. Um die Masterfunktion unter den einzelnen Controllern rotieren zu lassen bietet sich z. B. ein Verfahren an, dass eine ähnliche Funktion hat wie das Daisy-Chain-Verfahren. Sollte der Mastercontroller oder ein anderer Controller ausfallen, übernehmen die beiden übrigen Controller die Funktion. Dieses System hat den Vorteil, dass bei der Systemplanung beliebig viele Controller hinzugefügt werden können. Somit kann die Fehlertoleranz und die Ausfallsicherheit weiter gesteigert werden. Die Zuverlässigkeit dieses Verfahren lässt sich noch weiter erhöhen, wenn unterschiedliche Controller und unterschiedliche Software

11 Ein Latch-up (Latch-up-Effekt) bewirkt das ein Halbleiterübergang in einem Transistor niederohmig und somit leitend wird. Dieser Effekt kann zu einer Zerstörung des Chips oder wenigstens zu einem Fehlverhalten der Schaltung führt.

in unterschiedlichen Programmiersprachen verwendet werden (Abschnitt 2.3).
Dieser Aufwand zeigt jedoch auch die Schwäche des Systems. Um dieses System umzusetzen ist ein erheblicher Programmieraufwand erforderlich. An dieser stelle ist auch die Hardwareentwicklung nicht zu vernachlässigen, da alle Controller technisch in der Lage sein müssen miteinander zu kommunizieren. Ferner wird die zu erstellende Platine im Vergleich zum ersten Konzept wesentlich komplexer und größer sein.

3.6 Konzept 3: Duo-Duplex-Redundanz

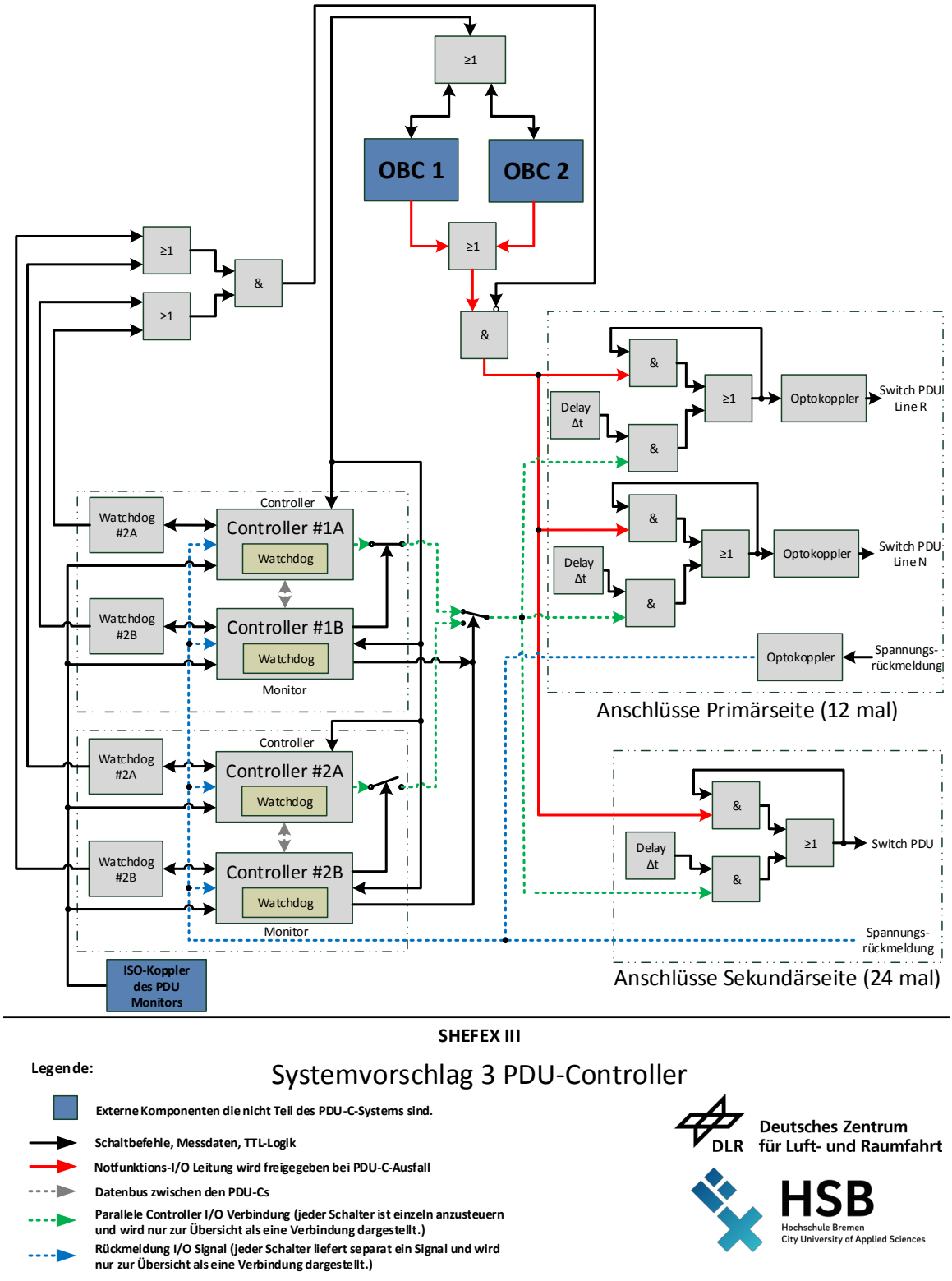


Abbildung 3.7: Konzept 3: Duo-Duplex-Redundanz [8, 31]

Das dritte Konzept ähnelt in einigen Teilen den vorangegangenen Konzepten (Illustration 3.5,3.6). Folglich werden die bereits erwähnten Punkte in diesem Teil nicht nochmals behandelt, da ihre Funktion identisch der im ersten Konzept ist.
Dazu gehören:

- OBCs
- PDU-Monitor
- Primär-Schalter
- Sekundär-Schalter
- OBC Notschaltung beim Ausfall des PDU-C

Das folgende Duo-Duplex-Konzept stammt aus einem Verkehrsflugzeug. Die Annahme, dass es sich um eine sicheres Konzept handelt, beruht auf der Tatsache das technische Anwendungen aus der Luftfahrt strengen Sicherheitsanforderungen unterliegen (Abschnitt 2.1).
Zu Beginn des PDU-C-Starts betätigt das Controller-Paar 1A und 1B die PDU-Schalter. Dabei bekommen beide Controller die identischen Daten und führen die gleichen Rechnungen aus. Der Controller 1B fungiert dabei jedoch nur als Monitor. Er vergleicht die Ergebnisse von Controller 1A mit seinen eigenen. Er selber jedoch keine Schaltbefehle aus. Kommt es nun zu einem Fehler, den der Monitor erkennt ist er in der Lage die Ausgänge des Master Controllers 1A stillzulegen und gleichzeitig auf das Controller-Paar 2A und 2B umzuschalten. Dieses Controller-Paar steht die gesamte Zeit in heißer Redundanz (Abschnitt 2.2.4) zur Verfügung und kann bei Bedarf sofort die Funktion übernehmen. Dem Controller-Paar 2A und 2B stehen nun die gleichen Möglichkeiten wie dem ersten Paar zur Verfügung. Wenn hierbei ein Fehler erkannt wird, ist es möglich, wieder zum ersten Paar zurückzuschalten. Dieses Paar kann möglicherweise seine Funktion durch einen Neustart wieder herstellen. Die Vorteile dieses Systems liegen in seiner Zuverlässigkeit. Es hat sein Qualifikation bereits in der Luftfahrt unter Beweis gestellt. Bei genauer Betrachtung fällt jedoch auf, dass ein Ausfall des Monitors dazuführen kann, dass ein Fehler im Master Controller A ggf. nicht erkannt wird. Es ist also notwendig die Schaltung weiter auszubauen. Zum Beispiel wäre es denkbar, den Watchdog des Monitors A mit an den Master A anzuschließen, damit Monitor A mit überwacht wird. Des Weiteren zeigt die Darstellung 3.7, dass es notwendig ist, den beiden Watchdogs eines Controller-Paar A oder B zusammen zu schalten. Betrachtet man die Controller-Paare als geschlossenes Subsystem führt der Ausfall eines Controllers egal, ob Monitor oder Master, zum Ausfall der gesamten Einheit. Ein Controller kann nicht gewährleisten, dass die Schaltbefehle korrekt sind. Somit gibt es im Vergleich zum zweiten Konzept, nur zwei Degradationsstufen anstatt drei. Dennoch ist dieses Entwurf interessant, da der Programmieraufwand vermutlich geringer ist, als im Konzept 2. Auch die Hardware ist ähnlich komplex. Es gibt zwar einen Controller mehr, jedoch nur noch zwei Controller, welche schalten. Der Wegfall der zu schaltenden Kanäle vereinfacht das Routing auf der Platine.

3.7 Fehlermöglichkeits- und -einflussanalyse Teil 2: Konzept Auswertung

Nach dem die Konzepte erstellt wurden, ist es notwendig, die FMEA ein zweites Mal durchzuführen. Teil der FMEA ist es, nachdem Schwachstellen identifiziert wurden und Gegenmaßnahmen ergriffen wurden, diese auf ihre Wirksamkeit hin zu untersuchen.
Die in Abbildung 3.8 dargestellte Analyse ist kürzer, als die voran gegangene (Abbildung 3.4). Die nun dargestellten möglichen Fehlerquellen sind die, die in der ersten FMEA rot umrahmt waren. Folglich wurden im zweiten Teil der FMEA nur die Fehler dargestellt, auf die durch ein PDU-C Konzept Einfluss genommen werden kann. Das Vereinfachen der Darstellung dient der besseren Übersichtlichkeit, die ursprüngliche Nummerierung wurde beibehalten um eine klare Zuordnung gewährleisten zu können.

Auswertung Konzept 1

HSB Hochschule Bremen City University of Applied Sciences — DLR

Produkt FMEA: SHEFEX III Konzept 1

Name / Abteilung: GNC | **Erstellt durch: Lars Johannsen** | **Datum: 15.06.2015**

					Ist Zustand							Verbesserter Zustand			
	Fehlerort / Fehlermerkmal	Potentielle Fehler	Fehlerfolge	Fehlerursache	A	B	E	RPZ	Empfohlene Maßnahmen	Verantwortlich	A	B	E	RPZ
2	Maschine	Unterbrechen der Energieversorgung des Navigationsystems	Ausfall des PDU-C	Auslösen einer Sicherung	3	7	4	84	beim Ausfall des PDU-C muss er weiterhin eine grundfunktionalität gegeben sein	PDU-C Konzept	3	7	4	84
5	Mensch	Falsche Bedienung	Es wird zuviel Energie beim Betrieb benötigt.	Nicht korrekt durchgeführte Prozeduren	3	7	6	126	Genaue Qualitätskontrollen durch die Fachabteilungen / exakte Schnittstellendefinition	Projektleitung / Fachabteilungen / PDU-C Konzept	1	6	2	12
9		Fehlerhafte Material Auswahl	Systemteile fallen beim Betrieb aus.	Bauteile sind nicht für die Umgebung geeignet	6	7	10	420	Für anfällige Komponenten ist immer eine Redundanz oder Degratation vorsehen	PDU-C Entwurf	6	6	5	180
12	Material	Materialermüdung	Timing-Probleme / Ausfall von Komponenten	Drift bauteilbezogener Größen	3	6	6	108	Verwendung von qualifizierten Bauteilen / Notbetrieb muss gewährleistet werden.	PDU-C Hardware / PDU-C Konzept / PDU Hardware	3	3	6	54
13			Überhitzung von Bauteilen	Starke Temperatur-schwankungen	5	8	9	360	Auf den Wirkungsgrad von Bauteilen achten / Konzept zum Wärmemanagement muss erstellt werden. Grundfunktionalität muss erhalten bleiben.	PDU-C Hardware / PDU Hardware / Konstruktion / PDU-C Konzept	4	8	7	224
14			Defekt von Systemen und mechanischen Strukturen	Mechanischer Schock	4	8	10	320	Bauteile müssen mechanische Belastungen ertragen / Notbetrieb muss gewährleistet werden.	PDU-C Hardware / PDU Hardware / Konstruktion / PDU-C Konzept	4	2	7	56
15		Materialfehler	Signalverlust / Kurzschluss	Elektrische Unterbrechung	4	3	10	120	QM für elektrische Verbindungen muss durchgeführt werden / Notbetrieb muss gewährleistet werden.	PDU-C Hardware / PDU-C Konzept	4	2	8	64
16			Systemausfall / Teilsystemausfall	Produktionsmängel bei Bauteilen	3	3	10	90	Qualifizierte Bauteile verwenden / Notbetrieb muss gewährleistet werden.	PDU-C Hardware / PDU-C Konzept	3	2	10	60
19	Umwelt	Hitze	Bauteilausfall durch Überhitzung	Keine Konvektion mangels Atmosphäre	5	4	10	200	Auf den Wirkungsgrad von Bauteilen achten / Konzept zum Wärme Management muss erstellt werden. Grundfunktionalität muss erhalten bleiben.	PDU-C Hardware / PDU Hardware / PDU C Konzept / GNC	5	4	5	100
20			Bauteilausfall durch Überhitzung / ggf. verglühen von Sensoren	Wiedereintritt	9	3	10	270	Auf den Wirkungsgrad von Bauteilen achten / Konzept zum Wärme Management muss erstellt werden. Grundfunktionalität muss erhalten bleiben.	PDU-C Hardware / PDU Hardware / PDU C Konzept	9	2	5	90
21		Vibration	Sensordrift / Teil Systemausfall	Wiedereintritt	9	8	1	72	Kontrolle der Messdaten auf Logik / Verwendung von Vibration unempfindlich Bauteilen	PDU-C Hardware / PDU Hardware / PDU C Konzept	9	5	1	45
22			Sensordrift / Teil Systemausfall	Launch	9	8	1	72	Kontrolle der Messdaten auf Logik / Verwendung von Vibration unempfindlich Bauteilen	PDU-C Hardware / PDU Hardware / PDU C Konzept	9	5	1	45
23	Methode	Timing	PDU-Kanäle haben einen undefinierten Zustand / Energieverbrauch ggf. zu hoch	Nicht aufeinander abgestimmt Schaltvorgänge	10	8	3	240	Durch das Schaltungsdesign Unterbinden von undefinierten Zuständen. Ausgiebige Tests sind notwendig	PDU-C Hardware / PDU Hardware / PDU C Konzept	2	5	3	30

Abbildung 3.8: FMEA Teil 2 des ersten Konzeptes

Die folgende Aufzählung gibt eine Erläuterung warum und wie die möglichen Fehler neu eingestuft wurden:

- **2. Auslösen einer Sicherung -** Da beim ersten Konzept weiterhin die beiden Versorgungsleitungen aus dem PDU zum PDU-C vorhanden sind und auch im PDU-C-System keine Unterverteilung, die abgesichert wird, vorhanden ist, bleibt die Beurteilung des Systems identisch. Eine mögliche Lösung für dieses Problem könnte sein, dass das PDU-C System intern weiter verzweigt wird, sodass die Schalter und der Controller nicht die gleichen Zuleitungen haben. Somit könnte im Fall eines Kurzschlusses des Controllers, zumindestens die Notfunktion über die OBCs gegeben sein. Es ist jedoch zu bedenken, dass die in der PDU vorgesehene Zuleitung des PDU-C bereits redundant sind (Abbildung 3.2). Ferner schafft man durch das Aufteilen der Energieversorgung im PDU-C System einen neuen Single Point of Failure. Um diesen zu beseitigen, müssen die getrennten Zuleitungen ebenfalls in zwei 1oo2 Schaltungen aufgeteilt werden. Es ist fraglich, ob dieser erhöhte Schaltungsaufwand zielführend ist. Des Weiteren muss dieses Vorgehen mit dem Entwickler der PDU abgestimmt sein.
- **5. Nicht korrekt durchgeführte Prozeduren -** Eine Kernaufgabe des PDU-Cs ist die Leistungsaufnahme des Navigationssystems im Moment des Einschaltens zu überwachen. Durch die Verwendung eines Controllers, der die Leistungsaufnahme überwacht, kann dieser Fehler weitetestgehend ausgeschlossen werden. Es ist zu beachten, dass bei steigender Komplexität des Funktionsumfangs ein ausführlicher Test der Software notwendig ist.
- **9. Bauteile sind nicht für die Umgebung geeignet -** Durch das Vorhandensein einer Notfunktionalität, ist der Wert für die Bedeutung und die Entdeckung eines Defektes gesunken. Dennoch führt der Ausfall des Controller oder des Watchdogs zu einer Reduzierung des Systems auf die Notfunktionen. Der Ausfall eines Schalters ist nicht folgenreich, da die Schalter schon redundant geplant worden sind. Somit wurden die Folgen dieses Fehlers zwar vermindert aber bleiben weiterhin potenziell hoch.
- **12. Drift bauteilbezogener Größen -** Dieses Problem kann nicht durch diesen PDU-C Entwurf beeinflusst werden. Dennoch kann das Risikos verhältnismäßig einfach gemindert werden. Dies wird im Abschnitt 3.8 genauer erläutert.
- **13. Starke Temperaturschwankungen -** Ähnlich wie bei Punkt 9, kann auf diesen Parameter nur minimal Einfluss genommen werden. Das Vorhandensein der Notfunktion durch die Einbindung der OBCs, vermindert jedoch die Auswirkungen und die Wahrscheinlichkeit des Entdeckens.
- **14. Mechanischer Schock -** Durch die Verwendung von geeigneten Bauteilen (Abschnitt 3.8) und das Vorhandensein einer sehr robusten Notfunktionalität sinkt die Bedeutung und eine Entdeckung wird wahrscheinlicher. Die Auswirkungen sind jedoch ähnlich geblieben. Weiterhin können Teile, die sich gelöst haben und die fehlende Kenntnis über die mechanische Belastungen, dieses potenzielle Problem schwer berechenbar machen.
- **15. Elektrische Unterbrechung -** Durch die Eigenständigkeit des Controllers ist der Verlust von Datenleitungen nicht notwendigerweise ein Problem. Durch eine entsprechende Prozedur im Fehlerfall kann ein Betrieb des PDU-C weiter gewährleistet werden. Der Verlust der Energiezufuhr durch einen Wackelkontakt oder eine schlechte Lötstelle ist

weiterhin ein potenzieller Fehler, der einen Systemausfall oder eine fehlerhafte Signalübertragung zur Folge hätte.

- **16. Produktionsmängel bei Bauteilen -** Durch die Notfunktion wurde die Bedeutung gesenkt, da Fehler nicht mehr so gravierend sind. Dennoch muss dieses Problem bei der Hardwareauswahl berücksichtigt werden.
- **19. Keine Konvektion mangels Atmosphäre -** Abermals hat die Notfunktion entschiedene Bedeutung für die Bewertung eines Problems. Auch die verwendete Hardware spielt hierbei eine Rolle. Durch die Verwendung von COTS-Komponenten kann das Problem jedoch nicht komplett ausgeschlossen werden. Ein Thermaltest wird Schwachstellen im Bereich Wärmeableitung jedoch aufzeigen können.
- **20. Wiedereintritt (Hitze) -** Die Auswirkungen dieses Fehlers sind weiterhin hoch. Durch den PDU-C werden die Werte für die Bedeutung und die Entdeckbarkeit verbessert. Durch den PDU-Monitor kann ein Kurzschluss oder ein erhöhter Energieverbrauch erkannt werden und der entsprechende Systemteil der Schaltung kann abgeschattet werden.
- **21.-22. Launch/Wiedereintritt (Vibration) -** Das Driften von Bauteilen kann durch eine PDU-C nicht behoben werden, jedoch führt das Vorhandensein der Notfunktion dazu, dass ein möglicher Fehler durch den Drift weniger Auswirkungen hat.
- **23. Nicht aufeinander abgestimmte Schaltvorgänge -** Das Vorhandensein eines Controllers, sowie der Möglichkeit zur Überwachung des Navigationssystems führt dazu, dass die Wahrscheinlichkeit des Auftretens, die Bedeutung und Entdeckungswahrscheinlichkeit verbessert werden. Dieses Problem kann durch den PDU-C sehr gut beeinflusst werden.

Auswertung Konzept 2

HSB Hochschule Bremen City University of Applied Sciences — DLR

Produkt FMEA: SHEFEX III Konzept 2

Name / Abteilung: GNC | **Erstellt durch: Lars Johannsen** | **Datum: 15.06.2015**

	Fehlerort / Fehlermerkmal	Potentielle Fehler	Fehlerfolge	Fehlerursache	Ist Zustand A	B	E	RPZ	Empfohlene Maßnahmen	Verantwortlich	Verbesserter Zustand A	B	E	RPZ
2	Maschine	Unterbrechen der Energieversorgung des Navigationsystems	Ausfall des PDU-C	Auslösen einer Sicherung	3	7	4	84	beim Ausfall des PDU-C muss er weiterhin eine grundfunktionalität gegeben sein	PDU-C Konzept	3	7	4	84
5	Mensch	Falsche Bedienung	Es wird zuviel Energie beim Betrieb benötigt.	Nicht korrekt durchgeführte Prozeduren	3	7	6	126	Genaue Qualitätskontrollen durch die Fachabteilungen / exakte Schnittstellendefinition	Projektleitung / Fachabteilungen / PDU-C Konzept	3	6	2	36
9		Fehlerhafte Material Auswahl	Systemteile fallen beim Betrieb aus.	Bauteile sind nicht für die Umgebung geeignet	6	7	10	420	Für anfällige Komponenten ist immer eine Redundanz oder Degratation vorsehen	PDU-C Entwurf	6	2	4	48
12	Material	Materialermüdung	Timing-Probleme / Ausfall von Komponenten	Drift bauteilbezogener Größen	3	6	6	108	Verwendung von qualifizierten Bauteilen / Notbetrieb muss gewährleistet werden.	PDU-C Hardware / PDU-C Konzept / PDU Hardware	3	3	6	54
13			Überhitzung von Bauteilen	Starke Temperatur-schwankungen	5	8	9	360	Auf den Wirkungsgrad von Bauteilen achten / Konzept zum Wärmemanagement muss erstellt werden. Grundfunktionalität muss erhalten bleiben.	PDU-C Hardware / PDU Hardware / Konstruktion / PDU-C Konzept	4	4	3	48
14			Defekt von Systemen und mechanischen Strukturen	Mechanischer Schock	4	8	10	320	Bauteile müssen mechanische Belastungen ertragen / Notbetrieb muss gewährleistet werden.	PDU-C Hardware / PDU Hardware / Konstruktion / PDU-C Konzept	4	2	6	48
15		Materialfehler	Signalverlust / Kurzschluss	Elektrische Unterbrechung	4	3	10	120	QM für elektrische Verbindungen muss durchgeführt werden / Notbetrieb muss gewährleistet werden.	PDU-C Hardware / PDU-C Konzept	4	2	8	64
16			Systemausfall / Teilsystemausfall	Produktionsmängel bei Bauteilen	3	3	10	90	Qualifizierte Bauteile verwenden / Notbetrieb muss gewährleistet werden.	PDU-C Hardware / PDU-C Konzept	3	1	3	9
19	Umwelt	Hitze	Bauteilausfall durch Überhitzung	Keine Konvektion mangels Atmosphäre	5	4	10	200	Auf den Wirkungsgrad von Bauteilen achten / Konzept zum Wärme Management muss erstellt werden. Grundfunktionalität muss erhalten bleiben.	PDU-C Hardware / PDU Hardware / PDU-C Konzept / GNC	5	2	5	50
20			Bauteilausfall durch Überhitzung / ggf. verglühen von Sensoren	Wiedereintritt	9	3	10	270	Auf den Wirkungsgrad von Bauteilen achten / Konzept zum Wärme Management muss erstellt werden. Grundfunktionalität muss erhalten bleiben.	PDU-C Hardware / PDU Hardware / PDU-C Konzept	9	2	5	90
21		Vibration	Sensordrift / Teil Systemausfall	Wiedereintritt	9	8	1	72	Kontrolle der Messdaten auf Logik / Verwendung von Vibration unempfindlich Bauteilen	PDU-C Hardware / PDU Hardware / PDU-C Konzept	7	3	1	21
22			Sensordrift / Teil Systemausfall	Launch	9	8	1	72	Kontrolle der Messdaten auf Logik / Verwendung von Vibration unempfindlich Bauteilen	PDU-C Hardware / PDU Hardware / PDU-C Konzept	7	3	1	21
23	Methode	Timing	PDU-Kanäle haben einen undefinierten Zustand / Energieverbrauch ggf. zu hoch	Nicht aufeinander abgestimmt Schaltvorgänge	10	8	3	240	Durch das Schaltungsdesign Unterbinden von undefinierten Zuständen. Ausgiebige Tests sind notwendig	PDU-C Hardware / PDU Hardware / PDU-C Konzept	2	5	3	30

Abbildung 3.9: FMEA Teil 2 des zweiten Konzeptes

Um eine bessere Übersichtlichkeit zu gewährleisten wird nachfolgend nur auf die Teile der FMEA eingegangen, die nicht identisch mit der bereits erarbeiteten ersten Teil der FMEA des ersten Konzeptes (Abbschnitt 3.7) sind. Die folgende Aufzählung gibt eine Erläuterung, aus welchem Grund und auf welche Weise die möglichen Fehler neu eingestuft wurden:

- **5. Nicht korrekt durchgeführte Prozeduren -** Durch die Redundanz des zweiten Konzeptes, wurden die Auswirkungen eines Fehlers gesenkt. Dabei ist auch die gegenseitige Überwachung der Controller von Bedeutung. Durch sie kann eine fehlerhafte Berechnung eines Controller detektiert werden und vermieden werden.
- **9. Bauteile sind nicht für die Umgebung geeignet -** Sollte ein Bauteil nicht für den Einsatz geeignet sein, hat ein Ausfall keine großen Auswirkung, da die folgenden Degradationsstufen seinen Ausfall kompensieren können. Sollten unterschiedliche Controller verwendet werden, sinkt das Risiko eine schlechte Auswahl getroffen zu haben nochmals.
- **13. Starke Temperaturschwankungen -** Durch die Verwendung unterschiedlicher Controller, sinkt die Wahrscheinlichkeit, dass alle Controller gleichzeitig ausfallen.
- **14. Mechanischer Schock -** Durch die Verwendung unterschiedlicher Controller sinkt die Wahrscheinlichkeit, dass alle Controller gleichzeitig ausfallen.

- **16. Produktionsmängel bei Bauteilen -** Es ist unwahrscheinlich, dass bei der Verwendung mehrere Controller, Mängel bei der Produktion aller Controller auftreten. Sind diese Bauteile zusätzlich noch von anderen Herstellen, ist dieser Fehler fast vollständig auszuschließen.
- **19. Keine Konvektion mangels Atmosphäre -** Abweichend vom ersten Konzept ist die Wahrscheinlichkeit geringer, dass es zu einem Systemausfall kommt, da drei Controller Pfade vorhanden sind anstelle von einem.
- **21.-22. Launch/Wiedereintritt (Vibration) -** Durch die Verwendung von komplexen Bauteilen, steigt die Wahrscheinlichkeit, dass diese anfällig sind für Vibrationen und somit z.B. für einen Drift. Es besteht zwar weiterhin die Möglichkeit, dass die Notfunktion in Kraft tritt. Jedoch steigt die Bedeutung des Problems weiterhin, da der gestiegene Systemumfang den den Umfang des Problems erhöht.

Auswertung Konzept 3

HSB Hochschule Bremen City University of Applied Sciences — DLR

Produkt FMEA: SHEFEX III Konzept 3

Name / Abteilung: GNC | **Erstellt durch: Lars Johannsen** | **Datum: 15.06.2015**

					Ist Zustand						Verbesserter Zustand			
	Fehlerort / Fehlermerkmal	Potentielle Fehler	Fehlerfolge	Fehlerursache	A	B	E	RPZ	Empfohlene Maßnahmen	Verantwortlich	A	B	E	RPZ
2	Maschine	Unterbrechen der Energieversorgung des Navigationsystems	Ausfall des PDU-C	Auslösen einer Sicherung	3	7	4	84	beim Ausfall des PDU-C muss er weiterhin eine grundfunktionalität gegeben sein	PDU-C Konzept	3	7	4	84
5	Mensch	Falsche Bedienung	Es wird zuviel Energie beim Betrieb benötigt.	Nicht korrekt durchgeführte Prozeduren	3	7	6	126	Genau Qualitätskontrollen durch die Fachgruppen / exakte Schnittstellendefinition	Projektleitung / Fachgruppen / PDU-C Konzept	3	6	2	36
9		Fehlerhafte Material Auswahl	Systemteile fallen beim Betrieb aus.	Bauteile sind nicht für die Umgebung geeignet	6	7	10	420	Für anfällige Komponenten ist immer eine Redundanz oder Degratation vorsehen	PDU-C Entwurf	7	2	4	56
12	Material	Materialermüdung	Timing-Probleme / Ausfall von Komponenten	Drift bauteilbezogener Größen	3	6	6	108	Verwendung von qualifizierten Bauteilen / Notbetrieb muss gewährleistet werden.	PDU-C Hardware / PDU-C Konzept / PDU Hardware	3	3	6	54
13			Überhitzung von Bauteilen	Starke Temperatur-schwankungen	5	8	9	360	Auf den Wirkungsgrad von Bauteilen achten / Konzept zum Wärmemanagement muss erstellt werden. Grundfunktionalität muss erhalten bleiben.	PDU-C Hardware / PDU Hardware / Konstruktion / PDU-C Konzept	4	4	3	48
14			Defekt von Systemen und mechanischen Strukturen	Mechanischer Schock	4	8	10	320	Bauteile müssen mechanische Belastungen ertragen / Notbetrieb muss gewährleistet werden.	PDU-C Hardware / PDU Hardware / Konstruktion / PDU-C Konzept	4	2	6	48
15		Materialfehler	Signalverlust / Kurzschluss	Elektrische Unterbrechung	4	3	10	120	QM für elektrische Verbindungen muss durchgeführt werden / Notbetrieb muss gewährleistet werden.	PDU-C Hardware / PDU-C Konzept	4	2	8	64
16			Systemausfall / Teilsystemausfall	Produktionsmängel bei Bauteilen	3	3	10	90	Qualifizierte Bauteile verwenden / Notbetrieb muss gewährleistet werden.	PDU-C Hardware / PDU-C Konzept	3	1	3	9
19	Umwelt	Hitze	Bauteilausfall durch Überhitzung	Keine Konvektion mangels Atmosphäre	5	4	10	200	Auf den Wirkungsgrad von Bauteilen achten / Konzept zum Wärme Management muss erstellt werden. Grundfunktionalität muss erhalten bleiben.	PDU-C Hardware / PDU Hardware / PDU-C Konzept / GNC	5	3	5	75
20			Bauteilausfall durch Überhitzung / ggf. verglühen von Sensoren	Wiedereintritt	9	3	10	270	Auf den Wirkungsgrad von Bauteilen achten / Konzept zum Wärme Management muss erstellt werden. Grundfunktionalität muss erhalten bleiben.	PDU-C Hardware / PDU Hardware / PDU-C Konzept	9	2	5	90
21		Vibration	Sensordrift / Teil Systemausfall	Wiedereintritt	9	8	1	72	Kontrolle der Messdaten auf Logik / Verwendung von Vibration unempfindlich Bauteilen	PDU-C Hardware / PDU Hardware / PDU-C Konzept	7	3	1	21
22			Sensordrift / Teil Systemausfall	Launch	9	8	1	72	Kontrolle der Messdaten auf Logik / Verwendung von Vibration unempfindlich Bauteilen	PDU-C Hardware / PDU Hardware / PDU-C Konzept	7	3	1	21
23	Methode	Timing	PDU-Kanäle haben einen undefinierten Zustand / Energieverbrauch ggf. zu hoch	Nicht aufeinander abgestimmt Schaltvorgänge	10	8	3	240	Durch das Schaltungsdesign Unterbinden von undefinierten Zuständen. Ausgiebige Tests sind notwendig	PDU-C Hardware / PDU Hardware / PDU-C Konzept	2	5	3	30

Abbildung 3.10: FMEA Teil 2 des dritten Konzeptes

Das dritte Konzept (Abschnitt 3.6) Unterscheidet sich nur in einem Punkt der FMEA vom zuvor genannten Konzept 2:

- **9.Bauteile sind nicht für die Umgebung geeignet -** Im Vergleich zum vorangegangenen Konzept besteht der Unterschied darin, dass es zwei redundante Mikrocontroller-Paare gibt. Im zweiten Konzept sind dagegen 3 redundante Mikrocontroller vorhanden. Dieser leichte Nachteil ist der Grund warum die Bewertung minimal schlechter ausfällt.
- **19. Keine Konvektion mangels Atmosphäre -** Abweichend vom zweiten Konzept ist die Wahrscheinlichkeit höher, dass es zu einem Systemausfall kommt da 2 Controller Pfade vorhanden sind anstelle von drei.

Zwischenfazit Konzeptvergleich

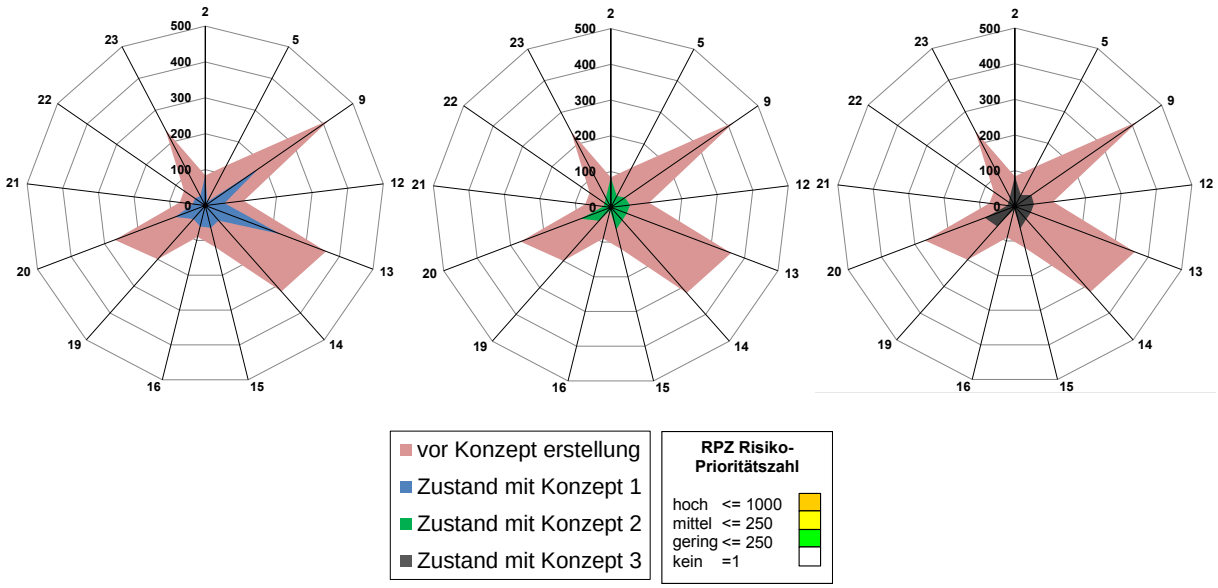


Abbildung 3.11: Vergleich zwischen dem ersten Teil der FMEA und dem zweiten Teil der FMEA

Betrachtet man die Abbildung 3.11 (Die Diagramme sind nochmal auf der beiliegen DVD enthalten) ist zu entnehmen, dass es zwischen dem Konzept 2 und dem Konzept 3 nur minimale Abweichungen gibt. Die gleiche Feststellung ist auch zu treffen, wenn man die Summen der drei FMEA in Tabelle 3.5 betrachtet.

Tabelle 3.5: RPZ Summen der vier durchgeführten FMEAs

Vergleich der RPZ Summen			
Ausgangszustand	**Konzept 1**	**Konzept 2**	**Konzept 3**
2482	1040	603	636

Aus diesem geringen Abstand der Zahlen von Konzept 2 und 3 ergibt sich nun anhand der Summe der Gesamtzahlen die Frage, aus welchem Grund diese beiden Werte dicht beieinander liegen, obwohl die Lösungen technisch unterschiedliche gestaltet sind. Betrachtet man nun den Beginn dieses Abschnitts 3.3, ist ersichtlich, dass die FMEA eine Fehlermöglichkeits- und -einflussanalyse ist und somit die Zuverlässigkeit bewertet. Es ist also nicht möglich, mit den bis jetzt in dieser Thesis angewendeten Techniken, eine Aussage über die Konzepte in Bezug auf Umsetzbarkeit und Zweckmäßigkeit zu treffen.
Um also ein Konzept auszuwählen, dass allen Anforderungen genügt, ist es notwendig noch weitere Informationen zu sammeln.

3.8 Auswahl von wesentlichen Hardwarekomponenten

Im Verlauf der Erstellung dieser Thesis hat sich ergeben, dass es notwendig ist, bestimmte Hardwarekomponenten festzulegen. Bestimmte Komponenten haben Einfluss auf die Gestaltung des Konzeptes und die Umsetzbarkeit des gesamten PDU-C Systems.
Generell ist es ratsam, bei der Hardwareentwicklung des gesamten PDU-Cs, auf die schon zuvor genannten COTS-Komponenten zurückzugreifen. Diese Entscheidung hat folgende Gründe:

- Auch wenn die Schlüsselkomponenten zu diesem Zeitpunkt noch nicht bestimmt sind, kann angenommen werden, dass wichtige Komponenten nicht Raumfahrt qualifiziert sein werden. Daraus resultiert, dass beim Entwurf der Schaltung auch andere nicht Raumfahrt qualifizierte Komponenten zum Einsatz kommen können.
- COTS-Komponenten sind wesentlich einfacher zu beschaffen.
- COTS-Komponenten sind erheblich billiger.
- Da es sich bei dem ersten Entwurf noch nicht um die finale Version der Platine handeln wird, kann das Budget geschont werden in dem herkömmliche Bauteile zum Einsatz kommen.
- Die für die Entwicklung benötigten Bauteil-Librarys für die Entwicklungssoftware sind nur schwer für Spezialteile zu bekommen und die Eigenentwicklung dieser Librarys benötigt Arbeitszeit.

Gleichwohl sollte bei der Entwicklung darauf geachtet werden, möglich wenig hochkomplexe IC's zu verwenden. Wenn die Möglichkeit besteht die Funktion des IC's mit Transistoren oder einfachen Schaltungselementen umzusetzen, dann ist dies die zu empfehlende Vorgehensweise. Somit wird die Möglichkeit bewahrt, im finalen Platinenentwurf möglichst viele Raumfahrt qualifizierte Komponenten verwenden zu können. Dies kann unterstützt werden, indem Bauteile mit identischen Packages Verwendung finden.

Ein wichtiges Bauteil ist der Taktgeber. Die in Controllern verbauten Taktgeber oder auch handelsüblichen Quarzoszillatoren sind empfindlich gegen Vibrationen. Die Störung kann dabei von leichten Abweichungen bis zum Ausfall des Quarzoszillators führen. Aus diesem Grund wird dingend dazu geraten, einen Quarzoszillator aus dem Raumfahrt- oder Militärbereich zu verwenden, bei dem diese Problematik nicht auftritt.

Ein weiterer wichtiger Schritt ist es die Controller Ein- und Ausgänge vor Überspannung, Kurzschlüssen, sowie elektromagnetischen Einflüssen zu schützen. Die meisten Controller besitzen intern einen solchen Schutz, dieser ist aber in der Regel nicht ausreichend um den Controller vollständig zu schützen.
Ein guter Schutz besteht aus zwei Widerständen von denen einer in Reihe und einer parallel zum Ausgang geschaltet sind. Zusätzlich geben zwei Z-Dioden, die parallel geschaltet werden einen Schutz vor Überspannung. Abschließend kann dann noch ein Kondensator parallel zum Controller Anschluss geschaltet werden. Die Auswahl der einzelnen Schutzmaßnahmen, hängt dabei vom Einsatzgebiet des Controllers und der Aufgabe des Anschlusses ab.

3.8.1 Controller Auswahl

Eine wichtige Komponente im PDU-C ist der Controller. Wie bereits in der Aufgabenstellung (Kapitel 1.1) beschrieben, stellen Einflüsse wie Strahlung, Vakuum, schnelle Abfolge von Druckwechseln, mechanischer Schock und starke Temperaturschwankungen besondere Anforderungen an die einzelnen Komponenten. Ferner gibt es noch die Anforderungen, dass das Bauteil kostengünstig, gut verfügbar, energiesparend und verhältnismäßig leicht zu programmieren sein sollte. Um nun einen Controller bestimmen zu können wird zunächst der Typ ausgewählt. Zur Auswahl stehen dabei Mikrocontroller, FPGA (Field Programmable Gate Array), Prozessoren (CPU) und ASICs (Anwendungsspezifische integrierte Schaltung). Bei dieser Auswahl fallen allerdings CPU und ASIC schon zu Beginn der Betrachtung als ungeeignet aus. Der entschiedene Vorteil von ASIC ist in diesem Anwendungsfall ein Nachteil. ASICs ermöglichen es, einen IC herstellen zu lassen, der genau den Vorstellungen das Auftraggebers entspricht. Es ist möglich, unterschiedliche Funktionen wie z. B. Mixed-Signal Schaltungen und analoge oder digitale Filter auf einem IC produzieren zulassen. Diese Anpassung der Schaltung führt dazu, dass ASICs in der Regel sehr schnell und energiesparend sind und gleichzeitig eine große Platzersparnis bringen. Gleichzeitig ist die Produktion eines Einzelstücks sehr teuer. Somit sind ASICs von Anfang an ausgeschlossen.
Handelsübliche CPUs hingegen sind relativ billig, haben jedoch den Nachteil, dass die Entwicklung eines PCB-Boards komplex ist. Somit wird eine Entwicklung sehr teuer. Ferner könnte so auf keinen Fall die Zuverlässigkeit des System gewährleistet werden. Folglich bleiben noch Mikrocontroller und FPGAs in der näheren Auswahl.
Die Tabelle 3.6 zeigt, dass die Vorteile und Nachteile von Mikrocontroller und FPGA in etwa gleich verteilt sind. Bei genauer Betrachtung fällt jedoch auf, dass die Vorteile des FPGAs im PDU-C nicht benötigt werden. Folglich fällt an dieser Stelle die Entscheidung, dass ein Mikrocontroller zum Einsatz kommen soll.

Tabelle 3.6: Vier Entscheidungsmerkmale für eine Auswahl zwischen Mikrocontroller und FPGA

	microC	**FPGA**	**Kommentar**
Kosten	+	-	Beispielsweise kostet der STM32F407VGT Microcontroller etwa 13€ und der FPGA Xilinx SPARTAN-6LX in etwa 20€.
Programmieraufwand	+	-	Der Programmieraufwand eines Mikrocontrollers ist geringer, es werden keine Hardwarebeschreibungssprachen benötigt.
Rechenleistung	-	+	Ein FPGA bietet die Möglichkeit hoher Rechenleistung bereitzustellen. Seine Stärken liegen in der Signalverarbeitung und dem variablen Konfigurierbarkeit und Einsetzbarkeit. Bei diesem Projekt sind die Stärken jedoch nicht von großer Bedeutung.
Raumfahrt qualifiziert	-	+	Es gibt raumfahrtqualifizierte FPGAs diese sind jedoch mit ca. 25.000 € pro Stück zu teuer, um zum Einsatz zu kommen.

Bei der Bestimmung eines Controller Models kommen erneut, die am Anfang des Abschnitts genannten, physischen Einflüsse zum Tragen. Darüber hinaus müssen auch, die durch die Schnittstellenbeschreibung von Kwiatkowski [17] gegebenen Anforderungen, betrachtet werden.
Eine durchgeführte Recherche ergab, dass sich zum Bearbeitungszeitpunkt dieser Bachelorthesis keine Raumfahrt qualifizierten Mikrocontroller auf dem Markt befinden. Ein weiteres Ergebnis dieser Recherche ergab, dass Mikrocontroller trozdem bei kleineren Satelliten oder Raumfahrtprojekten im Einsatz sind. Dabei waren vier Controller-Lösungen häufiger anzutreffen:

- Raspberry Pi
- Arduino
- Mikrocontroller ATmega128
- Mikrocontroller STM32F407

Der Raspberry Pi und das Arduino-Board wurden nicht weiter betrachtet, da es sich bei ihnen um ganze Einplatinencomputer handelt. Diese bringen mehr Hardware mit, als der PDU-C benötigt, welche nur zu einer größeren Fehlerwahrscheinlichkeit führt. Sie wurden an dieser Stelle trozdem der Vollständigkeit halber aufgeführt.
Bei einer weiterführenden Recherche konnte heraus gefunden werden, dass mit dem ATmega128 bereits bei Airbus Defence and Space ein Strahlungstest durchgeführt wurde [3]. Da dieser Test ein Novum im Bereich der Mikrocontroller ist, kommt dieser Controller möglicherweise vermehrt zum Einsatz. Ferner hat sich der ATmega128 durch eine einfach Programmierung und Robustheit etabliert.

Der Mikrocontroller STM32F407 hingegen ist neuer, aber trotzdem weit verbreitet. Ferner ist dieser Mikrocontroller bereits in mehreren Projekten des DLRs zum Einsatz gekommen. Darüber hinaus wurde auch dieser Controller bereits einer Strahlungsquelle im DLR ausgesetzt. Bei der Bestrahlung wurden 4 PCB-Boards mit dem STM32F407 bestückt und so programmiert, dass diese kontinuierlich Berechnungen durchführen. Bei der Bestrahlung der Mikrocontroller konnte beobachtet werden, dass dritte von 4 PCB-Boards die Bestrahlung funktionsfähig überstanden haben. Eine Untersuchung des defekten Boards hat ergeben, dass nicht der Controller defekt war, sondern der LDO (Low Drop-Out), der ihn mit Spannung versorgt hat. An dieser Stelle muss erwähnt werden, dass es sich bei der Bestrahlung des STM32F407 nicht um einen ausführlichen Test wie beim ATmega128 handelt. Der STM32F407 wurde während der Kalibrierung von Sensoren mit der dort verwendeten Strahlungsquelle ausgesetzt. Es wurde hierbei keine genaue Prozedur eingehalten oder die Strahlendosis ermittelt, der der Mikrocontroller ausgesetzt war. Somit lässt sich bei diesem nur sagen, dass er einmal einer Strahlungsquelle ausgesetzt war und danach die meisten der getesteten Mikrocontroller noch funktionsfähig waren. Aus diesem Grund wurden die erlangten Ergebnisse nicht weiter veröffentlicht.

Bei dem dritten Mikrocontroller wurden zur Bestimmung des Controllers abweichend zu den vorangegangenen Mikrocontrollern wie folgt vorgegangen. Zunächst wurden die äußeren Parameter der Mission betrachtet und ermittelt. Es wurde dabei darauf geachtet, welche Industriebereiche ähnliche Anforderungen an die Elektronik stellen, wie die Luft- und Raumfahrt. An dieser Stelle der Auswahl kann Bezug auf Normen-Recherche am Anfang dieser Thesis genommen werden. Bei dieser konnte festgestellt werden, dass der Automobilbereich ähnlich starke Anforderungen an die zu verwendende Elektronik stellt wie die Luft- und Raumfahrt. Die dort verwendeten

elektronischen Bauteile müssen resistent gegen Vibrationen, mechanische Schocks und Temperaturschwankungen sein. Unter diesen Gesichtspunkten fiel der Mikrocontroller TC1782 von Infineon als mögliche Komponente auf. Unter dem Markennamen PRO-SIL™bewirbt Infineon eine Kombination aus Mikrocontroller, Watchdog und Spannungsversorgung. Abhängig von Mikrocontroller und Watchdog gibt Infineon die in ISO 26262 beschriebenen Sicherheitsstufen ASIL B bis ASIL D an. Die Sicherheitsstufe ASIL D entspricht dabei einer Ausfallwahrscheinlichkeit von $< 10^{-8}$. In Verbindung mit der vorhandenen Notfallfunktion und der damit erhöhten Ausfallsicherheit, kann unter Umständen eine Ausfallwahrscheinlichkeit von $< 10^{-9}$ gewährleistet werden.
Des Weiteren spricht für die Wahl des TC 1782 seine Systemarchitektur. Er gehört zu einer Produktfamilie, die bei Infineon als TriCore™ bezeichnet wird. Anders als die Bezeichnung vermuten lässt, besitzt er keine drei Prozessorkerne sondern lediglich einen, sowie einer PCP-Einheit (Peripheral Control Processor) im Prozessor und dem externen Watchdog (Abbildung 3.12). Dabei funktioniert die PCP-Einheit als Monitor des Mikrocontrollerkerns. Somit ähnelt der Aufbau dem im Konzept 2 verwendeten Controller-Monitor-Paar.

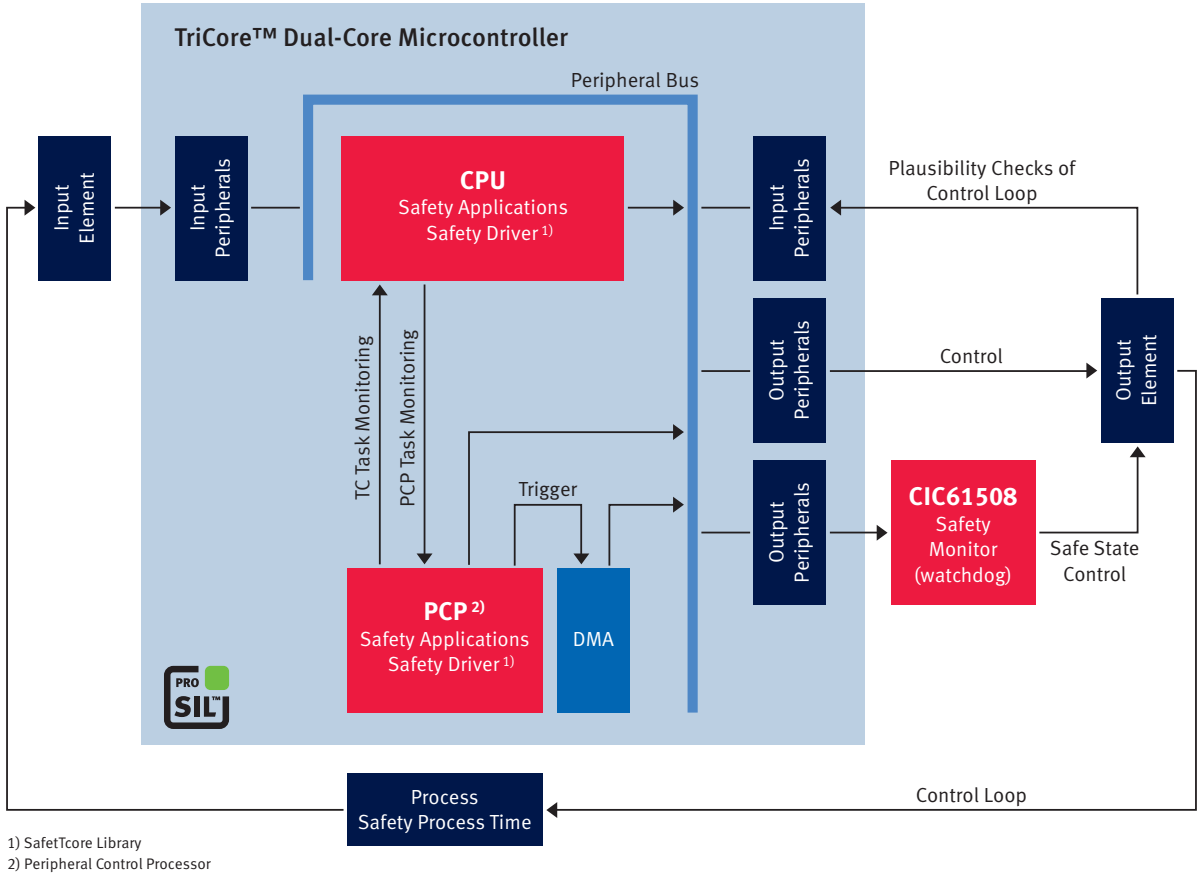


Abbildung 3.12: Interner Aufbau der TriCore™ Systemarchitektur Quelle:[1].

Tabelle 3.7: Darstellung der unterschiedlichen Entscheidungsmerkmale der drei zur Wahl stehenden Mikrocontroller.

Mikrocontroller	**STM32F407 VGT**	**ATmega128-AU16**	**TC1782**
GPIO Pins	136	53	88
rad-tolerant (getestet)	im DLR, jedoch nicht unter definierten Bedingungen	bei Astrium	nein
max Takt	168 MHz	16 MHz	180 MHz
Vorteil	ist am Standort in Benutzung	es gibt viel Dokumentation	sehr sicheres Konzept
Nachteil	es gibt noch keine verlässlichen Daten über die Strahlungsfestigkeit	zu wenig I/O Pins	keine Erfahrung mit diesem Mikrocontroller vorhanden

Der in der Tabelle 3.7 dargestellte Vergleich der drei zuvor genannten Mikrocontroller soll die für den PDU-C relevanten Merkmale hervorheben. Weitere Parameter, wie z. B. der für den Betrieb zugelassene Temperaturbereich, wurden ebenfalls anhand der Datenblätter miteinander verglichen. Dabei stellte sich heraus, dass alle Controller ähnliche Werte aufweisen und gleich geeignet sind und somit alle in Betracht gezogen werden können. Einzig der ATmega128 wies nur eine maximale Temperaturbeständigkeit von bis zu 85 °C auf, im Gegensatz von bis zu 125 °C bei den anderen beiden Controllern.

3.8.2 Auswahl eines Watchdog

Wie bereits zuvor beschrieben, ist die Auswahl des Watchdogs vom Einsatzfall abhängig. Im Fall des TC1782-Mikrocontrollers, ist die Auswahl verhältnismäßig einfach, da dieser bereits als Systemlösung mit dem Watchdog CIC61508 angeboten wird. Bei den anderen Mikrocontrollern ist die Auswahl schwieriger. Verwendet man den STM32F407 VGT, ist es notwendig, eine weitere Spannungsebene mit 3,3 V einzuführen, da der Mikrocontroller nicht mit 5 V sondern im Spannungsbereich 1,8 - 3,6 V betrieben werden muss. Ferner gibt es noch die Möglichkeit, die DC/DC Konverter in der PDU austauschen. Dabei muss allerdings auf die Spannungsversorgung der Peripherie im PDU-C System geachtet werden, da dort Aufgrund der TTL-Logik, 5 V benötigt werden.
Zur Überwachung der besagten zwei Spannungsebenen bieten sich Watchdogs an, die zusätzlich zum Heartbeat-Signal auch die beiden Spannungsebenen überwachen können. Auf diese Weise kann auch ein Defekt des Spannungswandlers mit detektiert werden. Für einen solchen Einsatzfall würde sich der LM3710 von Texas Instrument eignen. Beim Einsatz des ATmega128 würde sich ein UCC2946 oder ein MAX6746 eignen, da hier keine Überwachung von 2 Spannungsebenen benötigt wird.
Diese Auswahl zeigt allerdings auch, dass die Auswahl eines Watchdog stark von der Wahl der übrigen Komponenten abhängig ist. So ergibt sich, dass keine generelle Empfehlung für einen Watchdog gegeben werden kann. Trotzdem sei an dieser Stelle der Hinweis gegeben, dass sich Bauteile aus der Luftfahrt- oder Automobilindustrie anbieten würden.

Betrachtet man nun alle zuvor genannten Eigenschaften stellt sich heraus, dass unter dem Aspekt der Ausfallsicherheit der Mikrocontroller TC1782 mit der Watchdog CIC61508 und dem Spannungsregler TLE7368 die beste Wahl ist.

3.8.3 Physikalische Störeinflüsse

In der Luft- und Raumfahrt unterliegen elektronische Bauteile besonderen physikalischen Bedingungen. Zu diesen gehören Strahlung, Vakuum, schnelle Abfolge von Druckwechseln, mechanische Schocks und starke Temperaturschwankungen. Im Verlauf dieser Thesis wurde bereits vermehrt auf die diese Punkte eingegangen. Da diese Punkte allerdings eine besondere Bedeutung einnehmen, wird in diesem Unterabschnitt noch einmal zu jedem der zuvor genannten Punkte Bezug genommen.

Strahlung

Im Abschnitt „Auswahl von wichtigen Hardwarekomponenten“ wurden die Begriffe Strahlung und Raumfahrtqualifiziert verwendet ohne auf diese genauer einzugehen. Dies soll in dem nun folgenden Abschnitt nachgeholt werden. Ob ein Bauteil Strahlung verträgt und für die Raumfahrt qualifiziert ist, ist schwierig herauszufinden, da die Begriffe häufig umgangssprachlich verwendet werden, ohne hierbei genau definiert zu sein.
Man unterscheidet bei dem Begriff „strahlungsfest“ zwischen Radiation-Hardened (Rad-Hard) und Radiation-Tolerant. Wobei nur Bauteile, die Rad-Hard sind, wirklich Raumfahrt qualifiziert sind. Bei der Entwicklung von Rad-Hard Bauteilen wurde darauf geachtet, dass diese ausfallsicher gegen die meisten Arten von Strahlung sind. Rad-tolerante Komponenten werden wie herkömmliche Komponenten entwickelt und zeigen Ihre Tauglichkeit erst später im Betrieb. Dieser Unterschied kann wichtig sein, da Rad-Hard Bauteile unter Umständen Mechanismen zur Fehlererkennung und Behebung intern verbaut haben. In der Praxis ist es häufig so, dass Rad-Tolerante Bauteile bis zu einer Strahlung von 30 krad getestet sind. Strahlungsfeste Bauteile sind oft bis zu 150 krad getestet. Hier sind als Beispiel die Komponenten von Texas Instruments zu nennen. Eine genaue Definition, ab welchem Grenzwert ein Bauteil Rad-Hard oder Rad-Tollerant ist, kann nach ausgiebiger Recherche nicht getroffen werden.
Die Einheit wird dabei in rad angegeben. Dieses Einheitenzeichen ist allerdings veraltet, da es zu Verwechselungen mit der Winkeleinheit rad kommen kann. Aus diesem Grund ist das jetzt zu verwendende Einheitenzeichen rd. Die Einheit rd gilt in Deutschland nicht mehr als gesetzliche Einheit und wurde durch die SI-Einheit Gray abgelöst. Zwischen den Einheiten besteht folgender Zusammenhang [22]:

$$100\,\mathrm{rd} = 1\,\mathrm{Gy} = 1\,\frac{\mathrm{m}^2}{\mathrm{s}^2}$$

Ein weiteres Problem bei Strahlung ist , sie tritt im Weltraum nicht gleichmäßig auf. Die Strahlung variiert beispielsweise signifikant, je nach Höhe des Orbits. Darüber hinaus kommt es bei der Strahlung auf die Art, Größe und Energie der Partikel an. So können bei einer niedrigen

Strahlungskonzentration insgesamt trotzdem mehr Störungen auftreten, als bei einer größeren Strahlungskonzentration.

Für die Bauteilauswahl bedeutet, dass die Eignung eines Bauteils von seinem Einsatzgebiet im Weltraum abhängt. Im Fall des SHEFEX III PDU-C muss davon ausgegangen werden, dass kein Bauteil Strahlungsfest ist, da es sich bei den zu verwenden Bauteilen um COTS-Bauteile handelt und diese in der Regel nicht auf Strahlungsfestigkeit getestet wurden. Sollte im weiteren Verlauf des HNS-Navigationssystem Projektes eine Qualifizierung für Strahlungsfestigkeit des PDU-C gewünscht sein, muss dieses einem Strahlungstest unterzogen werden und gegebenenfalls Komponenten ausgetauscht werden.

Vakuum / schnelle Abfolge von Druckwechseln

Ähnlich wie bei der Strahlung kann bei COTS-Bauteilen keine Vakuumfestigkeit garantiert werden. Finden in elektronischen Bauteilen schnelle Druckwechsel statt, besteht die Gefahr das Lufteinschlüsse in den Bauteilen sich schlagartig ausdehnen oder komprimieren. Dieser Vorgang kann zu Beschädigungen im Bauteil führen und schlimmstenfalls das Bauteil komplett ausfallen lassen.
Bereits bei der Auswahl der Bauteile kann diesem Problem Rechnung getragen werden. Es sollte darauf verzichtet werden Bauteile mit einem flüssigen oder gasförmigen Inhalt zu verwenden. Zum Beispiel sind Elektrolytkondensatoren nicht für die Raumfahrt geeignet, Keramik hingegen schon. Ähnlich wie bei der Strahlung kann aber die Funktionsunfähig durch Tests in einer Thermal-Vakuumkammer überprüft werden.

Mechanischer Schock / Vibrationen

Wie bereits in diesem Kapitel erwähnt, wird empfohlen Bauteile aus dem Automobil-, Luftfahrt- oder Militärbereich zu verwenden. Diese zeichnen sich durch eine gute Robustheit gegenüber mechanischen Belastungen, sowie einer großen Toleranz gegen hohe und tiefe Temperaturen aus. Das alleine reicht allerdings nicht, um sicher zu stellen, dass es zu keinem Defekt bei den Bauteilen kommt. Die Frequenz der Vibration in der Raumfahrt ist eine andere als beispielsweise im Automobilbereich. Auch die mechanischen Schocks die durch das Absprengen einer Raketenstufe entstehen, können enorm sein. Aus diesem Grund ist es Empfehlenswert, diese mechanischen Eigenschaften auf einem Shaker zu überprüfen. Weitergehend ist es sinnvoll, bei der Erstellung des PCB-Boards einen Konstrukteur mit einzubinden, um eine mechanisch belastbare Befestigung zu entwickeln.

Temperaturschwankungen

Temperaturschwankungen können in der Raumfahrt durch unterschiedliche Quellen auftreten. Dazu gehören der Wiedereintritt in die Atmosphäre, der Wechsel zwischen Tag- und Nachtseite der Erde und die Erwärmung durch die eigene Elektronik. Dabei muss bedacht werden, dass es im Weltall kein Fluid gibt über die ein Wärmeaustausch erfolgen kann. Somit kann Wärme nur über mechanische Verbindungen, wie z. B. Befestigungen, Heatpipes, oder Infrarotstrahlung

abgegeben werden. Bei der Auswahl der Bauteile ist es also notwendig auf die Temperaturbeständigkeit zu achten. Durch die Verwendung von KFZ-Teilen ist dies geben, da sie häufig bei einer Umgebungstemperatur von 125 °C funktionsfähig bleiben. Des Weiteren muss der PDU-C mit in das Thermalkonzept des Navigationssystems bzw. von SHEFEX III mit eingebunden werden. Die Funktionsfähigkeit lässt sich abschließend in einer Thermal-Vakuumkammer überprüfen.

3.9 Risikoanalyse

Ähnlich wie die bereits durchgeführte FMEA dient die Risikoanalyse dazu Risiken zu erkennen und zu bewerten. Der Unterschied zwischen den beiden Analyseverfahren besteht in der Zielsetzung und ihrer Herkunft. Die FMEA stammt historisch aus dem technischen Bereichen der Automobil-, Luft- und Raumfahrtindustrie und dient dazu, technische Schwachstellen in einem System oder Prozess aufzudecken und Verbesserungen auf ihre Wirksamkeit hin zu untersuchen. Die Risikoanalyse ist hingegen häufiger im Projektmanagement vorzufinden und dient zum Aufspüren und Bewerten von organisatorischen Risiken, oberflächlichen, systematischen sowie Schnittstellenproblemen. Des Weiteren werden bei der Risikoanalyse getätigte Verbesserungsvorschläge nachfolgend nicht mehr auf ihre Wirksamkeit hin überprüft.

Der Vollständigkeit halber ist an dieser Stelle zu erwähnen, dass der Begriff Risikoanalyse sehr weitläufig ist und eine Vielzahl an Techniken und Methoden beinhaltet [5]. Die in diesem Fall gewählte Methode der Risikomatrix ist eine vergleichsweise einfache Methode. Ähnlich wie die FMEA ist sie sehr subjektiv, eignet sich aber gut um Probleme in Bezug zueinander Bewerten zu können. Die Tabelle 3.8 beinhaltet die möglichen Risiken und weist dabei auf Lösungsmöglichkeiten hin. Die aufgeführten Risiken sind zum Teil schon in der FMEA genannt worden. In der Risikoanalyse sind sie aus dem Blickwinkel eines Organisatoren zu betrachten. Die Abbildung 3.13 stellt die gleichen Risiken dar und setzt diese grafisch ins Verhältnis zueinander. Die in der Risikomatrix dargestellten Nummern entsprechen den in der Tabelle 3.8 verwendeten Nummerierung. Die durch die Risikoanalyse benannten und bewerteten Probleme werden im Abschnitt 3.10 zum auswählen eines Konzeptes verwendet.

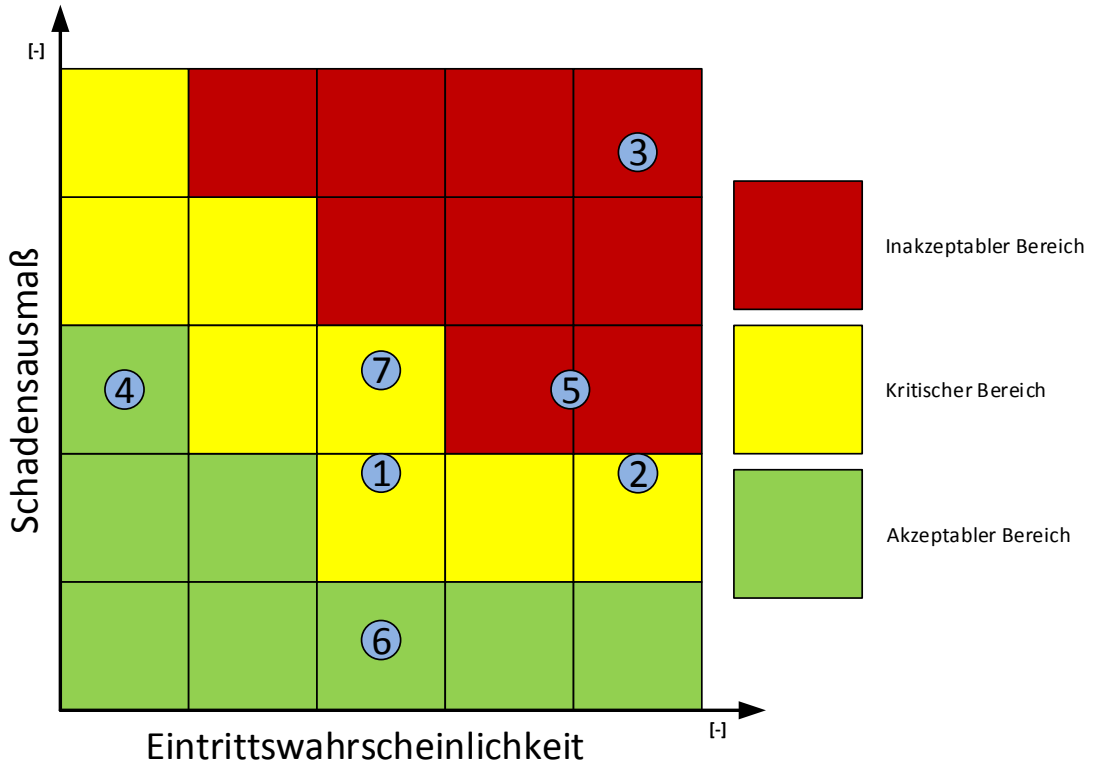


Abbildung 3.13: Bewertung der in Tabelle 3.8 benannten Risiken.

Tabelle 3.8: Organisatorische Risiken bei der PDU-C Entwicklung

Nummer	Risiko-beschreibung	Eintritts-wahrschein-lichkeit	Auswirkung	mögliche Strategie/Maßnahme	mögliche Anzeichen
1	Startup-Process des Navigationssystems ist zu komplex. Es kann zu schlecht detektierbaren Fehlern auf dem Launcher kommen.	mittel	Verzögerungen des Raketenstarts, was einen Finanzellen- und einen Imageschaden verursacht.	• Ein Fehlermanagement muss in der Software implementiert sein. Jeder Fehler der Auftritt muss durch eine Fehlermeldung **eindeutig** gekennzeichnet sein. • Eine exakte Schnittstellendefinition muss vorhanden sein. In der Dokumentation möglichst in Klartext ohne komplizierte Abkürzungen.	Die Wahrscheinlichkeit, dass der Fehler auftritt wird um so größer je weniger getestet wurde und je schlechter die Dokumentation ist.
2	Die Komplexität eines Systems erhöht die Fehleranfälligkeit	hoch	• Je komplexer das PDU-C System wird, um so schlechter lassen sich Faktoren wie z.B. Kosten- und Entwicklungsaufwand einschätzen. • Dies kann dazu führen, dass der Terminplan und das Projektbudget nicht eingehalten werden können.	Den Funktionsumfang einschränken. Dieser Vorgang sollte jedoch gezielt passieren und nicht automatisch durch eine Zeitlimitierung	Bereits am Anfang des Projektes übersteigen die Erstellung von Breadboard und Testsoftware die Zeitplanung erheblich.

Nummer	Risiko-beschreibung	Eintritts-wahrschein-lichkeit	Auswirkung	mögliche Strategie/Maßnahme	mögliche Anzeichen
3	Der Energiebedarf wurde bei der Planung nicht richtig ermittelt und ist somit für das Navigationssystem zu hoch	hoch	Das Navigationssystem kann unter Umständen nicht in diesem Projekt verwendet werden. Es entstehen somit kosten für eine externe Lösung	• Schaltungs- und Funktionsumfang so klein wie möglich gehalten werden. • Neuere Komponenten verwenden, diese sind zwar häufig nicht so robust doch oft Energiesparender.	Sehr viel Elektronik wird bei der Entwicklung verbaut. Der Energie bedarf kann schon bei der Entwicklung schlecht Geschätzt werden.
4	Bei dem Betrieb des Systems entsteht zu viel Wärme	niedrig	Defekt durch Überhitzung	Bei der Planung der Elektronik rechtzeitig einen Maschinenbau- oder Thermalingenieur.	Bei der Entwicklung der PCB Boards wird die mechanische Struktur nicht mit Berücksichtigt
5	Zeitaufwand für Test und Integration werden unterschätzt.	hoch	Die Testphase ist zu kurz und nötige Systemtests werden somit vernachlässigt.	Zeitpuffer für diesen Fall in der Projektplanung mit berücksichtigen.	Testkampagnen werden nicht mit berücksichtigt bei der Planung der Hardware.
6	Selten eingesetzte elektronische Bauteile haben lange Lieferzeiten.	mittel	Verzug im Zeitplan	• Meilensteine zum rechtzeitigen bestellen der Hardware sollten festgelegt werden. • Bei der Entwicklung der Schaltung auf die Verfügbarkeit der Teile achten.	Beim Hardwaredesign werden Kosten und Bezugsquelle nicht berücksichtigt.
7	Das PDU-C System wird zu groß.	mittel	Das entwickelte PDU-C passt nicht mehr in das System da es physisch zu groß ist	• Den Platzbedarf rechtzeitig Kalkulieren • Redesign der Schaltung • Einschränkung des Funktionsumfangs und damit auch der Schaltung	• Es gibt lange kein mechanisches Konzept • Die Form des Flugkörpers bleibt lange unbestimmt

3.10 Machbarkeitsbewertung und Konzept Auswahl

Die Machbarkeitsbewertung wird mit Hilfe eines morphologischen Kastens durchgeführt. Um die Bewertung durchführen zu können, werden die Ergebnisse der FMEA, Risikoanalyse und der Aufgabenstellung verwendet. Des Weiteren wird auf die Mikrocontrollerauswahl Bezug genommen und die Verwendung des Controllers mit dem ausgewählten Konzept erläutert.

Um die Eigenschaften der verschiedenen Konzepte besser vergleichen zu können, wurde eine Gewichtung (G) eingeführt. Diese sieht wie folgt aus:

- 1 = unwichtig
- 2 = eher unwichtig
- 3 = eher wichtig
- 4 = wichtig
- 5 = sehr wichtig

Anschließend wurden die Varianten im Rahmen der Richtlinie VDI 2225 wie folgt bewertet (B):

- 0 = unbefriedigend
- 1 = gerade noch tragbar
- 2 = ausreichend
- 3 = gut
- 4 = sehr gut

Um die Eignung der Konzepte zu bestimmen, wurde die technische Wertigkeit in der Tabelle 3.9 berechnet.

$$W_t = \frac{\textbf{Summe der Punkte je Variante}}{\textbf{Gesamtpunktzahl}} \tag{3.2}$$

$W_t > 0{,}8$ sehr gute Lösung
$W_t > 0{,}7$ gute Lösung
$W_t > 0{,}6$ schlechte Lösung

	Konzept 1	G	B	Konzept 2	G	B	Konzept 3	G	B
FMEA	ausreichend	5	3	sehr gut	5	5	gut	5	4
Risikoanalyse	ausreichend	3	2	ausreichend	3	2	ausreichend	3	2
Kosten	sehr gut	5	5	ungenügend	5	1	ausreichend	5	2
Sicherheit	ausreichend	5	2	sehr gut	5	5	gut	5	4
Platzbedarf	sehr gut	5	5	ungenügend	5	1	befriedigend	5	3
Aufwand	sehr gut	5	5	ungenügend	5	1	ausreichend	5	2
Leistungsaufnahme	gut	2	4	ausreichend	2	2	befriedigend	2	3
Einfehlertolleranz	ausreichend	4	3	sehr gut	4	5	gut	4	4
Start-up-Prozesses	sehr gut	5	5	sehr gut	5	5	sehr gut	5	5
intrinsisches degradationskoncept	befriedigend	4	3	sehr gut	4	5	gut	4	4
Erreichte Punktzahl			151			140			144
Maximale Punktzahl			200			200			200
Technische Wertigkeit			0,76			0,70			0,72
Legende	**Gewichtung**	**G**		**Bewertung**	**B**				

Tabelle 3.9: Morphologischer Kasten zur Bestimmung eines Konzeptes

Nachdem die technische Wertigkeit bestimmt wurde, ergibt sich, dass das Konzept 1 das am besten geeignete Konzept für das SHEFEX III Projekt bzw. das Navigationssystem ist. Das Ergebnis der Machbarkeitsbewertung ergibt allerdings das die technische Wertigkeit schlechter ist als 0,8. Folglich handelt es sich bei der Lösung um eine Gute und nicht um eine sehr gute Lösung. Dieses Ergebnis lässt sich drauf zurückführen, dass es sich bei dem Konzept 1 nicht um das Konzept mit einer optimalen Sicherheit handelt. In Anbetracht der Tatsache das die SHEFEX III Mission über unbewohntem Gebiet stattfindet, die Flugdauer sehr kurz ist und die Mission unbemannt ist, führt dies dazu, dass das Konzept trotzdem angenommen wird. Ein weiterer Grund für die Auswahl des Konzeptes 1 sind zudem die Kosten. Das Verwenden mehrerer Mikrocontroller zu einer zusätzlichen Belastung des knappen Energiebudgets. Ferner steigen auch die Kosten für die Entwicklung der Hardware und der Software.
Die Wertigkeit des Konzeptes 1 nimmt mit der Verwendung des Mikrocontrollers TC1782 noch zusätzlich zu. Durch die Eigenschaften des Mikrocontrollers in Kombination mit dem dazu gehörigen Watchdogs ergibt sich zum Mikrocontrollerkern noch eine Monitoring-Funktion der Berechnungsdaten des Mikrocontrollerkerns. Somit handelt es sich bei dieser Konstellation um eine Art Mischung zwischen Konzept 1 und Konzept 2.
Sollte dieses Navigationssystem weiterführend auch für andere Mission verwendet werden, muss darauf hingewiesen werden, dass es sich nicht dafür eignet in Systemen eingesetzt zu werden, in denen Menschen potenziell direkt oder indirekt gefährdet werden könnten. Das Konzept 1 ist nicht Ausfallsicher genug um die hierfür geforderten Anforderungen an die Fehlertoleranz zu erfüllen. Das hat zur Folge, dass für bemannte Missionen ein anderes Konzept verwendet werden muss. Betrachtet man nun die übrigen beiden Konzepte, dann fällt die Wahl auf das Konzept 3. Dieses Konzept ist fast genau so sicher wie Konzept 2 hat aber den Vorteil, dass der Aufwand bei der Programmierung geringer sein wird da die beiden primären Mikrocontroller nicht miteinander kommunizieren müssen und ferner eine Voter-Logik nicht benötigt wird.

4 Empfehlungen und Systembetrachtung

In diesem Abschnitt wird in komprimierter Form das Ergebnis dieser Bachelorthesis vorgestellt. Des Weiteren wird ein Ausblick auf weiterführende Arbeiten sowie Verbesserungsvorschläge gegeben.

4.1 Zusammenfassung

Die Aufgabenstellung dieser Bachelorthesis sah vor, dass ein Konzeptvorschlag für einen PDU-C zu entwickeln ist. Dabei sollte sich der PDU-C in das ein-fehlertolerante Navigationssystem einfügen. Darüber hinaus sollte der PDU-C in der Lage sein einen Start-Up-Prozess durchführen zu können. Nachdem dieser Prozess abgeschlossen ist, sollte der PDU-C die Möglichkeit bieten einzelne Sensoren wieder abzuschalten wenn eine Störung auftritt. Zusätzlich zu diesem Funktionsumfang musste der PDU-C so konzeptioniert sein, dass eine Funktionsstörung nicht zu einem Ausfall des Navigationssystems führen darf. Aus diesem Grund sollte der PDU-C ein intrinsisches Degradationskonzept zur Sicherstellung der Leistungsversorgung nach Ausfall des PDU-Cs besitzen. Dabei sollte schon während der Konzepterstellung die Hardware soweit mit bedacht werden, dass Schlüsselkomponenten identifiziert werden und Anforderungen, wie Strahlung, Vakuum, schnelle Abfolge von Druckwechseln, mechanischer Schock, starke Temperaturschwankungen, ein kleines Volumen und geringe Leistungsaufnahme, soweit wie möglich mit in die Planung einfließen.
Bei der Anfertigung dieser Bachelorthesis wurden diese Vorgaben bei der Konzepterstellung mit bedacht und erfüllt.
Zunächst wurden die möglichen Fehler eines solchen Systems ermittelt. Weiterführend wurden die zuvor erlangten Ergebnisse mit einer FMEA bewertet. Dieser Arbeitsschritt war notwendig um herauszufinden welche Fehlerquellen bei der Erstellung der Konzepte unbedingt beachtet werden müssen und welche Fehlerquellen durch andere Maßnahmen abgemindert werden können.
Mittels der drei im Anschluss entwickelten Konzepte wird versucht die gegebene Problemstellung durch unterschiedliche Ansätze bei der Controllerkonfiguration zu lösen. Nach diesem Schritt werden die Konzepte abermals in der FMEA betrachtet. Hierbei wird untersucht, welche Verbesserungen erreicht werden konnten. Dabei wurde festgestellt, dass das zweite und dritte Konzept mit einem geringen Unterschied die beiden Ausfallsichersten sind.
Da die Konzeptsicherheit alleine noch keine Aussage über die Machbarkeit zulässt, ist es notwendig gewesen weitere Betrachtungen des Problems durchzuführen. Zunächst wurden wichtige elektronische Schlüsselkomponenten definiert. Dabei wurden bei einigen Bauteilen Parameter bestimmt, die bei der Auswahl beachtet werden müssen. Zwei besonders wichtige Bauteile, wie der Mikrocontroller und der Watchdog, wurden direkt bestimmt. Dabei konnte der Mikrocontroller TC1782 und die Watchdog CIC61508 durch einen Auswahlprozess als die, für die gegebene Problemstellung am besten geeignetsten Bauteile identifiziert werden.
Darauf folgend wurde eine Risikoanalyse durchgeführt, diese dient dazu, weitere mögliche Fehlerquellen zu identifizieren, die durch organisatorische Maßnahmen positiv beeinflusst werden

können. Abschließend wurden für die Bestimmung eines tauglichen Konzeptes wichtige Parameter und die, durch voran gegangen Arbeitsschritte, erlangten Erkenntnisse in einem morphologischer Kasten zusammengefasst und ausgewertet. Die Vor- und Nachteile der einzelnen Konzepte sind in der Tabelle 4.1 aufgeführt.

Tabelle 4.1: Pro und Kontra der Konzepte

Konzept	Pro	Contra
Konzept 1	• Einfache Umsetzung • Verhältnismäßig geringe Kosten • Einfach zu programmieren • Geringer Platzbedarf	• Nur in Verbindung mit den OBCs ein-fehlertolerant • Ausfallsicherheit ausreichend aber nicht sehr gut
Konzept 2	• Sehr hohe Ausfallsicherheit • Das Einbringen von Diversität ist möglich • Ein-fehlertoleranz ist gegeben	• Sehr hohe Kosten • Sehr hoher Entwicklungsaufwand von Hard- und Software • Technisch schwere Umsetzbarkeit
Konzept 3	• Sehr hohe Ausfallsicherheit • Das Einbringen von Diversität ist möglich • Ein-fehlertoleranz ist gegeben	• Hohe Kosten • Hoher Entwicklungsaufwand von Hard- und Software

Abweichend vom Ergebnis der FMEA hat sich das Konzept 1 als die beste Lösung für die gegebene Problemstellung erwiesen. Es bietet den besten Kompromiss zwischen Zuverlässigkeit und Umsetzbarkeit. Durch die Verwendung nur eines Mikrocontrollers ist die Leistungsaufnahme geringer, als bei der Verwendung von drei Mikrocontrollern. Eine genauere Aussage zum Energieverbrauch kann zum jetzigen Zeitpunkt nicht getroffen werden. Die Bestimmung der Leistungsaufnahme des Mikrocontroller hängt stark von seiner Taktrate, sowie der Beschaltung der Ausgänge ab. Betrachtet man die Maximalwerte bei der Leistungsaufnahme bei den Mikrocontrollern, dann ist der ATmega128 der Sparsamste. Er ist aber auch im Vergleich der langsamste und der vom Funktionsumfang beschränkteste Mikrocontroller.

4.2 Ausblick

Die nun folgenden Punkte sind Empfehlungen und somit nicht notwendigerweise umzusetzen. Dabei liegt der Fokus in der Energieeinsparung und der Steigerung der Zuverlässigkeit.

Bei der Betrachtung des Konzeptes und der PDU von Kwiatkowski [17] fällt auf, dass die galvanische Trennung mit Rad-Hard Optokopplern umgesetzt werden soll. Das Problem besteht hier bei der Stromaufnahme der Optokoppler. Ein einfacher Optokoppler hat eine Stromaufnahme zwischen 5 – 20 mA. Multipliziert man den ungünstigsten Wert (IL74 Datenblatt auf der beiliegenden CD) mit der Anzahl der PDU-Schalter, ergibt sich die Stromaufnahme wie folgt:

$$\begin{aligned} I_{gesamt} &= I_{Optokoppler} \cdot Anzahl\,der\,Schalter \\ I_{gesamt} &= 20\,\text{mA} \cdot 36 \\ I_{gesamt} &= 720\,\text{mA} \end{aligned}$$

Hieraus ergibt sich ein großes, mögliches Einsparpotenzial. Verwendet man an Stelle des zuvor genannten Optokopplers einen TPL2361 von Toshiba wir nur ein Zwanzigstel des Stroms benötigt, um diesen zu beschalten. Gleichzeitig nimmt voraussichtlich auch die Zuverlässigkeit ab, da mehr Halbleiterelemente im Optokoppler verbaut sind. In der Praxis wird die Stromaufnahme der Optokoppler voraussichtlich nie die 720 mA erreichen, da es unwahrscheinlich ist, dass alle Schalter gleichzeitig betätigt werden bzw. einige von ihnen low-aktiv sind. Ein lohnendes Einsparpotenzial bleibt hier dennoch erhalten.

Eine weitere mögliche Änderung wäre es, die PDU Kanäle zu reduzieren, um so den Energieverbrauch weiter zu reduzieren. Weiterführend bietet sich hierdurch vielleicht sogar die Möglichkeit den Mikrocontroller ATmega128 zu verbauen und somit einen unter Strahlung getesteten Controller verwenden zu können.

Nachdem ein erster Schaltungsentwurf fertiggestellt wurde, sollte dieser auf seine Ausfallsicherheit hin untersucht werden. Dies kann mit den bereits beschrieben Techniken aus dem Abschnitt 2.2 durchgeführt werden oder mit nicht in dieser Arbeit näher beschriebenen Techniken wie beispielsweise der Fehlerbaumanalyse.

Es ist ratsam, nach dem Abschluss dieser Thesis, Testprozeduren zu erstellen. Auf diese Weise werden die Abläufe und Umgebungsparameter detaillierter definiert, wodurch es ggf. möglich ist weitere Anforderungen an den PDU-C im voraus zu identifizieren.

Der Prozess der Zuverlässigkeitsprüfung sollte während der gesamten SHEFEX III Projektlaufzeit weitergeführt werden, um so kontinuierlich eine Qualitätskontrolle durchführen zu können.

Ein wichtiger Punkt ist die Erstellung der benötigten Software für den PDU-C. Die Vergangenheit hat gezeigt, dass schwere Unfälle in der Luft- und Raumfahrt durch fehlerhafte Software verursacht werden können. Mit der Komplexität der Software, steigt die Gefahr des Auftretens eines Logikfehlers oder eines Programmierfehlers deutlich an. Es ist somit von großer Wichtigkeit eine umfassende Softwareplanung vorzunehmen und die Software ausgiebig zu testen. Zu diesem Zweck sollte die Norm DO-178C angewendet werden. Abhängig von der Sicherheitseinstufung des zu programmierenden Systems, erlaubt die DO-178C verschiedene Entwicklungsmethoden bzw. schreibt diese explizit vor.

Darüber hinaus muss im Zusammenhang mit der Softwareentwicklung auch das V-Modell erwähnt werden (Abbildung 4.1). Es schreibt einzelne Entwicklungsstufen vor, wobei jede Stufe in sich abgeschlossen ist, ferner bilden die Abschnitte mit ihren Ergebnissen konkrete Vorgaben für die Bearbeitung der nächste Stufe. So entstehen automatisch einzelne Planungsabschnitte, die gut dokumentiert werden können. Gleichzeitig steigt der Detaillierungsgrad der Planungsstufen, was bis zum eigentlichen Punkt der Programmierung weitergeführt wird. Nachfolgend singt der Detaillierungsgrad wieder, während die rechte Seite des V-Modells heraufsteigt. Die nun folgenden Stufen werden mit den jeweils gegenüberliegenden Stufen verglichen, um zu überprüfen, ob die entsprechenden Forderungen erfüllt wurden. Sollte ein Punkt bei der Kontrolle nicht erfüllt worden sein beginnt das V-Modell von vorne.

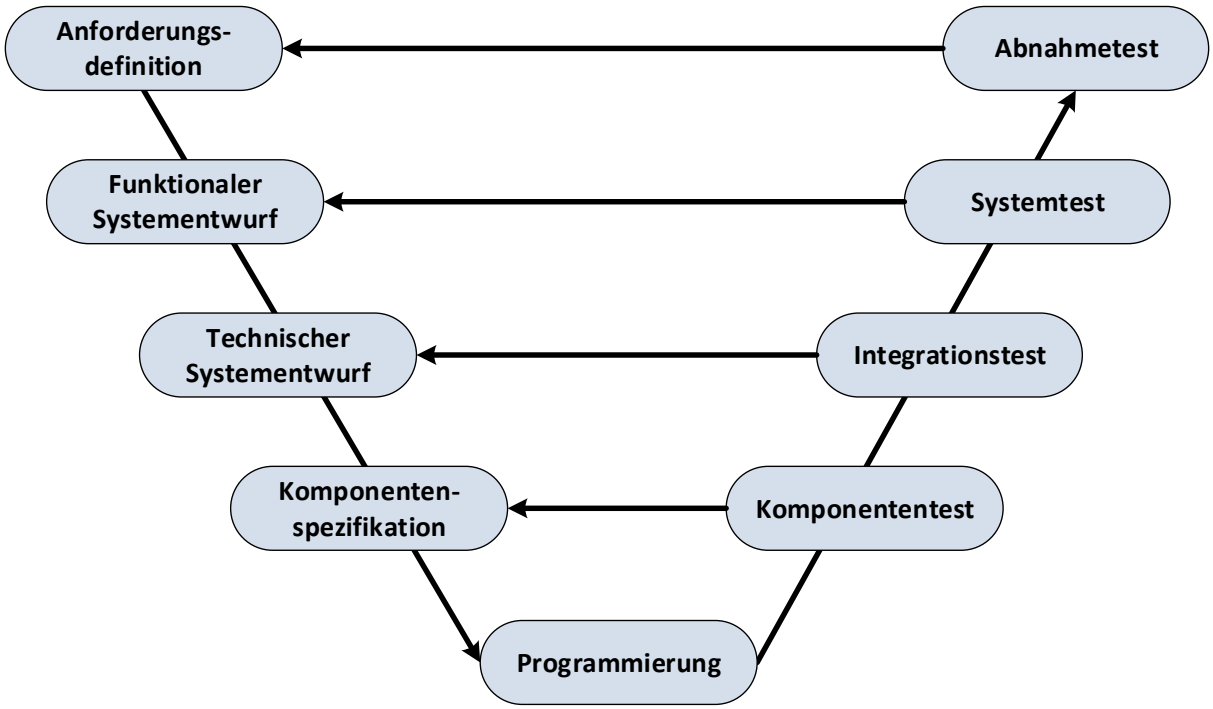


Abbildung 4.1: Exemplarische Darstellung eines V-Modells

Allgemein lässt sich sagen, dass die vorliegende Aufgabenstellung erfüllt worden ist. Die drei entwickelten Konzepte sind alle in der Lage, die Ausfallsicherheitsanforderungen zu erfüllen.
Das Ergebnis lässt allerdings noch keine endgültige Schlussfolgerung zur Zuverlässigkeit zu, da für eine detaillierte Betrachtung eine konkrete Schaltung benötigt wird. Das Erstellen und Prüfen dieser Schaltung stellt eine arbeits- und zeitintensive Aufgabe dar, die in einer weiteren Abschlussarbeit bearbeitet und gelöst werden könnte.

A Literaturverzeichnis

[1] Infineon Technologies AG. *TriCore™and CIC61508 Powerful Safety Computing Platform*. Sep. 2011.

[2] Siemens AG. *Funktionale Sicherheit in der Prozessinstrumentierung mit Einstufung SIL Fragen, Beispiele, Hintergründe*. Apr. 2007.

[3] C.Daniel A.Schüttauf S.Rakers. „Radiation Effects Data Workshop (REDW), 2010 IEEE“. In: *Radiation test of 8 bit Microcontrollers ATmega128 & AT90CAN128*. Hrsg. von C.Daniel A.Schüttauf S.Rakers. IEEE, Juli 2010, S. 3.

[4] Alessandro Birolini. *Zuverlässigkeit von Geräten und Systemen*. 4. Aufl. Berlin: Springer, 1997. ISBN: 3540609970.

[5] Claudia Cottin und Sebastian D hler. *Risikoanalyse: Modellierung, Beurteilung und Management von Risiken mit Praxisbeispielen*. 2. Auflage. StudienbuÃàcher Wirtschaftsmathematik. Wiesbaden: Springer, 2013. ISBN: 9783658008307.

[6] ECSS00. *ECSS-S-ST-00C Description, implementation and general requirements*. European Cooperation for Space Standardization, 2008.

[7] ECSS40. *ECSS-Q-40A Sicherheits*. S.27. Deutsches Zentrum für Luft- und Raumfahrt e.V., 2009.

[8] Holger Flühr. *Avionik und Flugsicherungstechnik: Einführung in Kommunikationstechnik, Navigation, Surveillance*. 2., erweiterte Aufl. 2012. Berlin: Springer, 2012. ISBN: 9783642335761.

[9] Dr. Patrick Fritz. *FMEA Vorlagen*. Deutsch. Fachhochschule Vorarlberg. Nov. 2013. URL: www.hochleistungsorganisation.com.

[10] Vera Gebhardt. *Funktionale Sicherheit nach ISO 26262 : ein Praxisleitfaden zur Umsetzung*. 1. Aufl. Safari Tech Books Online. Heidelberg: dpunkt-Verl., 2013.

[11] Riedel GmbH. *Vorgehen bei der Durchführung der FMEA-Gefahrenanalyse*. 2009.

[12] Karl-Erwin Groflpietsch Hubert Kirrmann. „Fehlertolerante Steuerungs- und Regelungssysteme“. In: *at - Automatisierungstechnik Band 50, Heft 8/2002* (2002).

[13] *IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems*. International Electrotechnical Commission, 1998-2000.

[14] SAE International. *ARP 4761: Guidelines and Methods for Conducting the Safety Assessment on Civil Airborne Systems and Equipment*. Warrendale. 1996.

[15] Lars Johannsen und Renè Schwarz. *EXPOSÉ ZUR BACHELORTHESIS: Erarbeitung eines Konzeptes zur aktiven Steuerung einer hochzuverlässigen Leistungsversorgungseinheit für ein hybrides Navigationssystem*. März 2015.

[16] Bodo Kälble und Rolf Reudenbach. *Sichere Maschinen in Europa : Risikobeurteilung und Sicherheitskonzept*. 5. überarb. Aufl., Mai 2012. Bd. Teil 3. Sichere Maschinen in Europa ; Teil 3. Bochum: DC Verl., 2012.

[17] Norbert Kwiatkowski. „Entwicklung eines Referenzdesigns einer hochverfügbaren Leistungsversorgungseinheit für das SHEFEX III-Navigationssystem“. Bachelorthesis. Jade Hochschule, 2014.

[18] John C. Leveson und Knight; Nancy G. *An experimental evalution of the Assumption of independence in multi-version programming*. 1986.

[19] Peter L w, Roland Pabst und Erwin Petry. *Funktionale Sicherheit in der Praxis: Anwendung von DIN EN 61508 und ISO/DIS 26262 bei der Entwicklung von Serienprodukten*. 1. Aufl. Heidelberg: dpunkt-Verl., 2010. ISBN: 9783898645706.

[20] *Maschinenrichtlinie Richtlinie 2006/42/EG*. Das Europäische Parlament und der Rat der Europäischen Union, 2006.

[21] Heinrich Mensen. *Betrieb und Technik von Verkehrsflugzeugen*. Heidelberg: Springer, 2012. ISBN: 9783540687405.

[22] Fran ois Cardarelli und M.J. Shields. *Encyclopaedia of scientific units, weights and measures: their SI equivalences and origins*. London [u.a.]: Springer, 2003. ISBN: 185233682X.

[23] Horst Radermacher. „Explosion nach sechs Sekunden“. In: *FAZ.NET* (Oktober 2014).

[24] Kristina Radzeviciute. „Evaluation und Entwicklung von Bewertungsmodellen für die funktionale Sicherheit von elektronischen/elektrischen Systemen“. Diplomarbeit. Otto-Friedrich-Universität Bamberg, 2009.

[25] Konrad Reif. *Automobilelektronik: Eine Einführhrung für Ingenieure ; mit 38 Tabellen*. 4., überarbeitete Auflage. ATZ/MTZ-Fachbuch. Wiesbaden: Vieweg+Teubner Verlag, 2012. ISBN: 9783834886583.

[26] David A. Rennels u. a. „Fault-Tolerant Systems, 1997. Proceedings., Pacific Rim International Symposium on“. In: *A fault-tolerant embedded microcontroller testbed*. University of California at Los Angeles. IEEE, Dezember 1997.

[27] René Schwarz und Stephan Theil. „A Fault-Tolerant On-Board Computing and Data Handling Architecture Incorporating a Concept for Failure Detection, Isolation, and Recovery for the SHEFEX III Navigation System“. In: *Proceedings of the 13th International Conference on Space Operations (SpaceOps), May 5–9, 2014, Pasadena, California*. American Institute of Aeronautics und Astronautics (AIAA), Mai 2014.

[28] Daniel AJ Sokolov. „Explodierte US-Rakete: Wer soll das bezahlen?“ In: *heise online* (Mai 2015). URL: http://heise.de/-2651535.

[29] European Cooperation For Space Standardization. *ECSS-Q-ST-30-02C Space product assurance - Failure modes, effects (and criticality) analysis (FMEA/FMECA)*. English. ECSS European Cooperation for Space Standardization, März 2009.

[30] Thorsten Tietjen, AndrË Decker und Dieter H.M¸ller. *FMEA Praxis: das Komplettpaket für Training und Anwendung*. 3., ¸berarbeitete Auflage. M¸nchen: Hanser, 2011. ISBN: 9783446402676.

[31] Pascal Traverse, Isabelle Lacaze und Jean Souyris. „Airbus Fly-By-Wire: A Total Approach To Dependability“. In: *IFIP International Federation for Information Processing* 156 (2004), S. 191–212.

[32] VDA. *Band 4: Produkt- und Prozess-FMEA*. VDA, 2006.

[33] Kahle Waltraud und Liebscher Eckhard. *Zuverlässigkeitsanalyse und Qualitätssicherung*. Berlin, Boston: Oldenbourg Verlag, 2013.

[34] Martin Werdich. *FMEA - Einführung und Moderation: Durch systematische Entwicklung zur übersichtlichen Risikominimierung (inkl. Methoden im Umfeld)*. 2., überarb. und verb. Aufl. 2012. Wiesbaden: Vieweg+Teubner Verlag, 2012. ISBN: 9783834822178.